MILITARY HANDBOOK

SYSTEM SAFETY ENGINEERING DESIGN GUIDE FOR ARMY MATERIEL

AMSC N/A

AREA SAFT

FOREWORD

1. This military handbook is approved for use by all Activities and Agencies of the Department of the Army and is available for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this document should be addressed to: Director, US Army AMC Field Safety Activity, ATTN: AMXOS-SE, Charlestown, IN 47111-9669, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. This handbook was developed under the auspices of the US Army Materiel Command's Engineering Design Handbook Program, which is under the direction of the US Army Management Engineering College. Research Triangle Institute was the prime contractor for the preparation of this handbook, which was prepared under Contract No. DAAG34-73-C-0051.

CONTENTS

PART ONE
SYSTEM SAFETY

CHAPTER 1
INTRODUCTION TO SYSTEM SAFETY

CONTENTS (cont'd)

CHAPTER 2
SAFETY ENGINEERING CONCEPTS AND OBJECTIVES

APPENDIX 2A
EXAMPLES OF SAFETY TRADEOFF STUDIES

CONTENTS (cont'd)

PART TWO
SYSTEM SAFETY ANALYSES

CHAPTER 3
INTRODUCTION TO ANALYSIS

CHAPTER 4
PRELIMINARY HAZARD ANALYSIS

CONTENTS (cont'd)

APPENDIX 4A
INFORMATION SOURCES FOR SAFETY DATA AND RELIABILITY DATA

CHAPTER 5
SUBSYSTEM HAZARD ANALYSIS

CONTENTS (cont'd)

CHAPTER 6
SYSTEM HAZARD ANALYSIS

CONTENTS (cont'd)

CHAPTER 7
SOFTWARE ANALYSIS

CHAPTER 8
OPERATING AND SUPPORT HAZARD ANALYSIS

CONTENTS (cont'd)

PART THREE
GENERAL DESIGN REQUIREMENTS

CHAPTER 9
CONSIDERATIONS FOR GENERAL DESIGN APPLICATIONS

CONTENTS (cont'd)

CHAPTER 10
HAZARDS

CONTENTS (cont'd)

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (cont'd)

LIST OF ILLUSTRATIONS (cont'd)

LIST OF TABLES

LIST OF TABLES (cont'd)

LIST OF ABBREVIATIONS AND ACRONYMS

ACGIH = American Conference of Governmental Industrial Hygienists
AEL = accessible emission limit
AFALC = Air Force Acquisition Logistics Center
AIR = American Institute of Research
AMC = US Army Materiel Command
AIT = autoignition temperature
AMSAA = US Army Materiel Systems Analysis Activity
ANSI = American National Standards Institute
AOAP = Army Oil Analysis Program
APDS = armor-piercing discarding sabot
AR = Army Regulation
ASARC = Army System Acquisition Review Council
ASME = American Society of Mechanical Engineers
ASMIS = Army Safety Management Information System
ASP = automated sneak program
ATE = automatic test equipment
BIT = built-in test
BITE = built-in test equipment
BRH = Bureau of Radiological Health
C_t = time concentration factor
CA = criticality analysis
CDR = Critical Design Review
CFR = Code of Federal Regulations
CO = carbon monoxide
CO_2 = carbon dioxide
$COCl_2$ = phosgene
CPR = cardiopulmonary resuscitation
CW = continuous wave
D_t = dosage factor
DA = Department of the Army
DAB = Defense Acquisition Board
DARCOM = US Army Materiel Development and Readiness Command (now US Army Materiel Command (AMC))
DB = dry-bulb
DID = data item description
DoD = Department of Defense
DOT = US Department of Transportation
DTIC = Defense Technical Information Center
EBW = exploding bridgewire
ED = effective dose
ED_{50} = dosage necessary to produce a particular effect in 50% of an infinite population of test animals

EHF = extremely high frequency
EIR = equipment improvement report
EL = exposure limit
EMF = electromotive force
EMI = electromagnetic interference
EOD = Explosive Ordnance Disposal
EPA = US Environmental Protection Agency
ET = effective temperature
FHA = fault hazard analysis
FMEA = failure mode and effects analysis
FMECA = failure mode, effects, and criticality analysis
FSD = full-scale development
FTA = fault tree analysis
FTCA = Federal Torts Claims Act
GFCI = ground fault circuit interrupter
GFE = Government-furnished equipment
GFP = Government-furnished property
GOCO = Government-owned, contractor-operated
Hb = hemoglobin
HCl = hydrogen chloride
HCN = hydrogen cyanide
HEL = US Army Human Engineering Laboratory
HEP = high-explosive plastic
HERO = hazards of electromagnetic radiation to ordnance
HF = high frequency
HPR = human performance reliability
H_2S = hydrogen sulfide
I = incapacitating
IC_{50} = incapacitating concentration factor
IFVS = infantry fighting vehicle system
ILS = integrated logistic support
IPR = in-process review
IR = infrared
JAN = Joint Army and Navy
L = lethal
LD = lethal dose
LD_{50} = statistical estimate of the dosage necessary to kill 50% of an infinite population of test animals
LF = low frequency
LFL = lower flammability limit
LOS = line of sight
MA = managing activity
MAC = maximum allowable concentration

MADP = Materiel Acquisition Decision Process
MANPRINT = Manpower and Personnel Integration
MEOP = maximum expected operating pressure
MF = medium frequency
MICOM = US Army Missile Command
MIL-STD = military standard
MPE = maximum permissible exposure
MRSA = US Army Materiel Readiness Support Activity
NASA = National Aeronautics and Space Administration
NBC = nuclear, biological, and chemical
NCRP = National Council on Radiation Protection
NEC = National Electrical Code
NFPA = National Fire Protection Association
NIOSH = National Institute of Occupational Safety and Health
NRC = Nuclear Regulatory Commission
NSCCA = nuclear safety cross-check analysis
O&S = operating and support
O&SHA = operating and support hazard analysis
OD = optical density
OHA = operating hazard analysis
OSHA = Occupational Safety and Health Administration
PDR = Preliminary Design Review
PAM = pamphlet
PEF = personnel-equipment functional
PHA = preliminary hazard analysis
PM = program manager
ppm = parts per million
PRF = pulse repetition frequency
PSIL-4 = preferred speech interference level
QDR = Quality Deficiency Report
R = roentgen
rad = radiation absorbed dose
rbe = relative biological effectiveness
rem = roentgen equivalent man
RF = radio frequency

RFNA = red fuming nitric acid
RFP = request for proposal
ROC = required operational capability
S&A = safing and arming
SAE = Society of Automotive Engineers
SCA = sneak circuit analysis
SDC = sample data collection
SHA = system hazard analysis
SHF = super high frequency
SIT = spontaneous ignition temperature
SOAP = Spectrometric Oil Analysis Program
SOC = self-organizing concept
SPC = system performance report
SPL = sound-pressure level
SSA = software sneak analysis
SSHA = subsystem hazard analysis
SSPP = System Safety Program Plan
STEL = short-term exposure limit
T_L = lower temperature limit
TAMMS = The Army Maintenance Management System
TB = technical bulletins
TECOM = US Army Test and Evaluation Command
THERP = technique for human error rate prediction
TLV = threshold limit value
TMTT = tell me three times
TOP = test operation procedure
TRISAFE = triple redundancy incorporating self-adaptive failure exclusion
UDMH = unsymmetrical dimethyl hydrazine
UFL = upper flammability limit
USAEHA = US Army Environmental Hygiene Agency
USASC = US Army Safety Center
UHF = ultrahigh frequency
VHF = very high frequency
VLF = very low frequency
WB = wet-bulb
WBGT = wet-bulb global temperature

PART ONE
SYSTEM SAFETY
CHAPTER 1
INTRODUCTION TO SYSTEM SAFETY

This chapter, which provides an initial overview of system safety within the US Army, begins by contrasting the obsolete principles that have guided the safety policies of the Army in the past with the up-to-date principles that guide the policies of today. This is followed by a brief history of how system safety as a discipline evolved in the US Army. Product liability—one of the most powerful factors influencing system safety today—is discussed next. The system safety program requirements are addressed. The chapter closes with a discussion of the relationship of system safety to other disciplines involved in the acquisition of materiel for the US Army.

1-1 PHILOSOPHY

The military profession has never been considered safe. In fact, many people join the Armed Forces to be held in esteem for exhibiting daring and courage in the face of the enemy. Unfortunately, the enemy is not the only source of death or injury faced by the soldier; his own equipment can kill him just as easily. For example, members of the Ancient and Honorable Order of Artillerymen were admired for their willingness to work with primitive cannon, which frequently exploded with devastating results. Gradually, commanders realized that losses of personnel and equipment through accidents were just as final and as serious as losses caused by enemy action.

As the complexity of Army systems increased, the possibility of accidents increased too. Also the increased lethality of some Army systems increased the magnitude of adverse effects should an accident occur. These and other factors, such as weapon system and training costs, increased the need for accident prevention.

1-1.1 OUTDATED CONCEPTS OF ARMY ACCIDENT CAUSES

This increased need for safety led to a reexamination of the causes and prevention of accidents within the Army. This reexamination revealed that many long-standing concepts about accident causes were fallacious. A discussion of some of these fallacies follows:

1. Fallacy Number 1:

a. *Fallacy.* Operator errors are the cause of most accidents. The remaining few accidents are due to "Acts of God" or equipment failures. Therefore, preventing accidents, investigating accidents, and administering punishment for involvement in accidents are command functions. Thus the occurrence or absence of accidents is an indication of the competence of the commander.

b. *Discussion.* Reexamination of safety concepts indicated that the causes of accidents often originated long before the personnel of a unit received or were trained on the equipment. Deficiencies in equipment design or production were found to be powerful causal factors that often had gone unnoticed because they did not cause accidents until the equipment was fielded. In addition, mistakes by maintenance personnel set the stage for accidents that were not the fault of the operators. In some cases accidents were caused by operator error, but in many other instances the accidents should not have been attributed to mistakes by operators. Thus the concept of "operator error" as it was—i.e., when an operator was involved in an accident, it was usually his fault—had to be modified.

2. Fallacy Number 2:

a. *Fallacy.* Safety problems of a new piece of equipment can be identified only after a prototype has been built or the equipment has entered service.

b. *Discussion.* New methods permit early safety analysis to evaluate potential safety problems in a new piece of equipment before the design of the system is begun. This new safety analysis capability is part of a systematic program that will ultimately result in safer equipment, fewer accidents, and less need for costly modifications.

3. Fallacy Number 3:

a. *Fallacy.* Safer equipment always costs more.

b. *Discussion.* In some cases the safer design is the cheaper one—even when viewed only in the narrow frame of hardware procurement costs. For example, the Army switched from liquid propellant missiles to solid propellant ones, which are both safer and cheaper. This is an important example of a higher degree of safety for less cost. In other cases the safer design may cost exactly the same—again considering only the hardware procurement costs. A discussion in Chapter 9 will illustrate how a valve oriented in one direction in a line would be "fail-safe",

although the same valve oriented in the opposite direction could lead to an accident. Even when design changes for increased safety do increase the initial procurement cost of the hardware, they will probably decrease the life cycle costs of the system because safer design will probably lengthen the average useful life of the system and will yield decreased operating and maintenance personnel training costs, lower repair parts use, and lower depot or factory rebuild costs.

4. Fallacy Number 4:

a. *Fallacy*. Safety slows operation.

b. *Discussion*. With safer equipment less operational time is lost through accidents; therefore, the need to involve other personnel and equipment in corrective activities is eliminated. Equipment that is inherently safe or is made safe through proper design features helps speed operations because operators do not have to follow elaborate procedures that are required when equipment is known to be unsafe.

1-1.2 SYSTEM SAFETY POLICY AND FUNDAMENTAL CONCEPTS

The policy statements regarding the Army Safety Program contained in Army Regulation (AR) 385-10 (Ref. 1) include the following statement:

"Available resources must be applied against hazards on a 'worst-first' basis. Evaluation of hazard priority must include consideration of the overall potential consequences defined by degree of injury, occupational illness, and damage. Mission, legal, and statutory implications of each hazardous situation must also be considered.".

From the general policy statements concerning system safety, fundamental system safety concepts have evolved. Some of these concepts follow:

1. Strong management interest in system safety and emphasis on its accomplishments are necessary to produce a safe system.

2. A hazardous condition is a necessary prerequisite for an accident to occur. Hazardous conditions may be classified as hazardous characteristics of a system, product, operation, or location; equipment malfunctions; or adverse environmental effects. If a specific hazardous condition is eliminated, no accident can result from it. If the condition cannot be eliminated but can be adequately controlled, the probability of an accident will at least be reduced.

3. Poor consideration of human factors can result in operator errors that can cause accidents. Whenever possible, equipment should be designed to minimize the chance of operator error. If the chances of human error cannot be removed from the equipment through design, then extensive training must be given to the operators in the correct operation of the equipment.

4. To minimize design or production defects in a cost-effective manner, system safety programs must be initiated early in the acquisition process.

5. An inherently safe system should be the primary goal of every designer.

1-2 HISTORY

System safety as an applied discipline is new to the military. For centuries the cannon served as an outstanding example of an unsafe military design. Over the years accidents with cannon were reduced but not as the result of an organized system safety program. Improvements were made in the cannon to improve range, projectile weight, and cannon life, and these improvements resulted in a safer weapon. The lack of an organization concerned with system safety prevented the lessons learned regarding the cannon from being applied to other procurement programs. An action took place in 1958 that led to the establishment of system safety organizations.

"On 22 May 1958, a major accident at a NIKE-AJAX air defense site near Middletown, NJ, resulted in extensive property damage and loss of lives to Army personnel. An Ad Hoc Committee, appointed by the Army's Chief of Ordnance, was assembled to study the findings of the Board of Investigation and to identify '...areas where improvement in organization, mission, assignments and procedures would enhance the safety and reliability of the overall missile system programs of the Ordnance Corps.' Among the recommendations resulting from this special study were the following:

"...a. That safety control through independent review and a balanced technical check of missile systems be established to prevent compromise of safe design and operations in the rush to perform mandatory engineering accomplishments...

"...b. That the Army (Ordnance) Missile Command establish an authoritative safety organization to review missile weapons systems design...

"Based on these recommendations, a formal system safety engineering organization was created at Redstone Arsenal in July 1960; the basic mission of this organization was to ensure that safety engineering requirements, consistent with operational utilization, be incorporated into the weapon system's design. This organization became the first system safety activity within the Department of the Army.

"...In 1963, MICOM [US Army Missile Command] briefed the Department of the Army Safety Director's conference on the benefits being derived from our efforts and recommended adoption of similar programs at the other commodity commands. Soon thereafter, the first AR 385-16, 'System Safety', was published by DA, based upon a draft prepared by our office. The Army System Safety Program had begun." (Ref. 2).

In 1963 the Department of Defense (DoD) also recognized the need for guidance regarding system safety and

issued military specification MIL-S-38130, *General Requirements for Safety Engineering and Associated Subsystems and Equipment*, for all Services and for all types of equipment. Later it was decided that the requirements for system safety programs were better suited to a military standard (MIL-STD). Therefore, MIL-S-38130 was replaced by MIL-STD-882 (Ref. 3) in 1969.

Since 1963, the Army has devoted continuing attention to all aspects of system safety, and safety training programs are continually refined. Consideration of the safety budget is an important part of the procurement planning process. New and improved safety regulations, standards, and specifications have been developed to guide the safety program of the Army. DoD and Army directives, instructions, standards, and regulations covering safety are discussed in par. 1-4.

Having reviewed briefly the history of system safety, let us next examine one of the most potent forces shaping the present and future impact of system safety—the effects of product liability on the US Army.

1-3 PRODUCT LIABILITY

Product liability is the general term indicating that manufacturers and sellers of products that prove to be defective are liable for personal injuries to or damage to the property of those using the products. Product liability is not new, but the legal precedents during the last 25 yr have made this concept a very popular remedy in the US courts. The previously rigid requirements for proving the contractor's liability in injury or damage cases have been eased; consequently, new liability cases are now being reported everyday. The justification is that the costs of injuries in liability cases should be borne by the manufacturers and sellers of the defective products, rather than by the persons injured (Refs. 4 and 5). This great increase in the number of liability court cases is supported by a situation accepted as fact, namely, that some manufacturers produce unsafe products. Judgments and settlements for very large sums are common.

The discussion that follows will explain why, for military equipment, the Government may be required to reimburse the contractor for any of his liability losses. However, because of the 27 June 1988 Supreme Court decision—discussed in par. 1-3.2—military and other Government contractors now have broad immunity against such losses. Product liability as well as the fact that safer equipment contributes to operational capability are the reasons that Army materiel contracts contain requirements for contractor safety programs.

1-3.1 THE CONTRACTOR AND THE GOVERNMENT

As a sovereign power, the United States Government cannot be sued without its consent. The Government has never given its consent for any suits to be brought under any concept of product liability (Ref. 6). Why then is this an area of concern in the Army acquisition process? The interest is financial because under all cost-type contracts the Government agrees to indemnify (repay for loss) the contractor for any damages he may be required to pay as a result of litigation or settlement. Therefore, although the Army contractor is the named defendant in a liability case, any award probably will be paid out of the US Treasury. The cost of Army equipment that is proved defective in a successful product liability suit will therefore include payments to reimburse the contractor.

In cases that involve a design developed by a contractor to satisfy the requirements of a functional Army specification, the liability of the Government may be limited. Without a clearly stated indemnity clause, argument must be made by the contractor that some specific requirement of the contract—i.e., specification, material, Government-furnished equipment (GFE), or other factor—was the root cause of the product defect that caused the injury. This issue becomes more clouded because if the cause of the defect were obvious, the contractor would have had the legal duty to bring it to the Army's attention.

1-3.1.1 Special Contractor Exposure

Some contractors are producing Army equipment that is manufactured to specific, detailed, Army-provided manufacturing specifications. The exact design of the equipment is a contractual requirement to be fulfilled by the contractor. Should this manufactured item be the cause of injury to anyone—a Government civilian, a military person, or a private citizen—he can sue the contractor. The type of relief to the contractor through reimbursement by the Government depends on the type of indemnification clause in the contract.

1-3.1.2 Relaxing the Immunity of the Government

The Federal Torts Claims Act (FTCA) of 1946 provides for litigation of tort* claims in the Federal District Courts. There are certain necessary conditions that must be present to create a liability under the FTCA. The most important of these elements is that the situation or act in question was under Government control. Claimants seeking recovery under FTCA have advanced many theories of Government control. Some of these theories follow:

"A. *Contractual Provisions.* The safety provisions contained in a Government contract have greatly influenced Government liability. Typical provisions of a Government contract dealing with hazardous activities, such as explosives manufacture, provide for Government safety inspections in compliance with Government safety manuals standards and permit work stoppage if standards are not met. The contract additionally may require

---

*A tort is a breach of duty to exercise due care.

specified materials, designs and construction procedures to be used. Such provisions can place the Government in control of contract operations for safety purposes and can make the Government liable for accidents involving the contractor's employees.

"B. *Good Samaritan Doctrine*. Government liability may arise by the Government performing duties in connection with a contract which it is not obliged to perform. Government employees nearly always volunteer suggestions or recommendations to the contractor which comments concern for safety conditions. This principle may be illustrated by the ancient story of the blind man crossing the street. If a bystander simply observes the blind man threading his way through traffic across a busy street, he is not responsible for an accident to the blind person. On the other hand if he voluntarily assumes to help the blind man across the street he immediately comes under a duty to perform his guidance with reasonable care.

"C. Another theory by which the Government is held liable is based upon the *Ownership of the Premises Where the Contract is Performed*. The law in most states provides that the owner of real property must take certain steps to protect the interest of persons invited on to the land for business purposes. The owner must exercise reasonable care to protect the safety of such persons. This includes a duty to keep the premises in safe condition and to warn visitors of concealed perils of which the owner knows or should know; i.e., GOCO [Government-owned, contractor-operated] operations, Government ranges, etc.

"D. The next theory: *Ownership of Materials Utilized in the Contract's Performance*. Aside from the ownership of the premises upon which the contract is being performed, it is possible to base a claim against the Government on injuries caused by Government property utilized in a contract's performance.

"E. The next theory is *Non-delegable Duties as to Ultra-Hazardous Acts*. Absolute liability can arise irrespective of how the Tort Feasor conducts himself; it is imposed automatically when any damages are incurred as a result of the decision to engage in a dangerous or ultra-hazardous activity.

"F. The next theory concerns *Discretionary Acts*. This theory provides that there shall not be any liability imposed when: 'any claim based upon an act or omission of any employee of the Government based upon the exercise or performance...of discretion in any function or duty...whether or not the discretion involved be abused.' There has been general agreement that high level policy decisions cannot result in liability. Where, however, the decision occurs at the 'operational' level of governmental activity, which is to say, when it is made by one who is actively engaged in carrying out the work in the field, there have been cases declaring that the Government is liable for its acts or omissions.

"G. Another theory that has been utilized is *Res Ipsa Loquitor*. This doctrine makes it impossible to sue the Government under the FTCA without proving the negligence of a specific employee. The cases applying this doctrine typically list the following requirements for its use:

(1) The instrumentality causing harm was within the exclusive control of a Government employee.

(2) The Government employee was acting within the scope of his employment.

(3) The accident would not have occurred under normal circumstances and in the absence of negligence by those in control. In a Government contract situation, however, it is often difficult to show sufficient control by either party where both the Government and contractor have partial control over the instrumentality allegedly causing the claimant's injury.

"H. Finally there is the theory of *Employment of an Incompetent Contractor*." (Ref. 6)

1-3.2 CONTRACTOR AND GOVERNMENT LIABILITY AND THE MILITARY PERSON

In past years the courts ruled that not only civilian but also military personnel can sue manufacturers of equipment responsible for injuries. Although the Government was still immune from suit unless immunity was waived, the contractor providing systems or services was open to direct suit when his products or services caused injury.

The courts were concerned that the safety features of a military system may be inadequate or faulty, and the defense that a person in the military assumes risks with regard to the use of equipment not assumed by a civilian was no longer allowed. The courts have stated that in order for a military person to assume risk, he must be aware of the danger (identification of specific hazards), and he must have a voluntary choice whether or not to encounter the hazards. This consideration required knowledge and appreciation of the risk as well as the voluntary choice to encounter it. A 27 June 1988 Supreme Court decision, however, in the case of Marine copilot Boyle versus United Technologies changed the liability responsibilities. The decision gave the military and other Government contractors broad immunity against liability for deaths and injuries to service members and others when caused by negligently designed equipment. This decision was a major victory for the military equipment industry, which had been deluged in recent years with dozens of suits by injured military personnel and survivors of dead personnel. Under the Supreme Court ruling, manufacturers of aircraft, ground vehicles, and other equipment cannot be held responsible for mishaps involving the items when they have followed design and production specifications established by US Government agencies. The opinion was based on the position that an

exemption to normal liability rules is justified for Government contractors engaged in balancing the safety and combat effectiveness of systems and equipment.

1-3.3 THE ROLE OF SYSTEM SAFETY IN PRODUCT LIABILITY

Government attorneys and others are identifying the alarming growth of the liability problem. These people point out that if the equipment procured by the Army were free of defects, there would be no injuries from defects, and product liability litigation would not be an Army problem. How can the Army approach this goal of having defect-free equipment?

The foundation upon which to build defect-free Army systems is a good product assurance program and a well-integrated system safety program. Fortunately, more and more contractors recognize that the best protection against product liability is strict attention to the safety and quality of their products and the adequacy of their safety support. The basis for an expectation of success in such a program must be the commitment by high-level management to develop, produce and sell only high-quality, safe products. Army materiel acquisition personnel must be committed to insisting upon this objective. To be effective, this policy must be communicated to every person who is involved in the Army acquisition process.

Good safety support in the Army acquisition process starts with adequate consideration for safety during concept exploration and continues throughout the acquisition process. In the fielded system complete disclosure of remaining hazards must be provided in warnings. Instructions for operation, maintenance, or repair of the equipment must also identify the dangers involved in performing these activities incorrectly. Anticipating foreseeable misuse of Army equipment can become as important as identifying the hazards due to normal use (Ref. 5).

1-3.4 PRODUCT LIABILITY SUMMARY

No binding rules regarding product liability can be stated since each liability case is decided on its own merit. Some generalized conclusions concerning product liability and the military are presented in this subparagraph. These conclusions should be considered by developers of Army materiel. In addition, Army procurement personnel should seek competent legal advice in every case concerning product liability since court decisions change the legal precedents rather often.

The conclusions follow:

1. An injured person, whether a military or civilian Government employee or a member of the public at large, may not sue the US Government for injuries because of the combined effects of the theory of "sovereign immunity", the Federal Employees' Compensation Act, and the separate statutory system for compensation of military personnel.

2. An injured person may sue any person or institution other than the Government, including individual Government employees, co-workers, or contractor companies. The principle of strict liability—the legal concept wherein the defendant is liable without regard to fault or negligence—applies equally to companies manufacturing and distributing products to civilian consumers. This right of action does not include the right of one military person to sue another when both are performing their official duties. However, if either military person is acting outside the scope of his employment, with respect to any action for damages, he is then treated as a member of the public at large and may be held liable.

3. The Federal Tort Claims Act of 1946 makes the Government liable for injuries to third persons (those persons outside the Government). This statute provides for third person recovery for injuries due to the negligent and wrongful act or omission of any Government employee while acting within the scope of his employment. It operates in the same manner and to the same extent as a private individual is responsible under like circumstances (Ref. 4).

4. Although the Army contractually requires equipment manufacturers to have system safety programs and although the Army accepts the equipment, the manufacturer is legally responsible under strict liability concepts to produce only safe products or services. A Government employee, whether civilian or military, may sue the company selling the equipment that caused the injury. This is a general statement; the execution of individual procurement contracts requires specific advice from competent legal counsel as previously stated.

5. Sometimes the intended military use of a product requires that a safety feature present in a civilian version of the product be eliminated. When this action is taken by the managing activity, it may insulate the manufacturer from liability when there is an injury that would have been prevented by the eliminated safety feature. If the manufacturer is exempt from payment in such cases, the Government will be paying the awards for damages. Of course, it is important that the managing activity be aware of any safety alteration to an "off-the-shelf" purchase for military use.

1-4 SYSTEM SAFETY PROGRAM REQUIREMENTS

The need for system safety programs has been recognized at all command levels of the Department of Defense, the Department of the Army, and the other military departments. Regulations, directives, and military standards have created the Army Safety Program philosophy, objectives, concepts, and operating guidelines, which will be described briefly in the paragraphs that follow. Since the system safety requirements are found in documents issued by various headquarters, the

discussion in the paragraphs that follow will be developed around these various documents.

System safety documents that relate to occupational safety or nuclear safety are not included in this discussion for the following reasons:

1. The field of occupational safety does overlap some of the system safety activities, but it is not primarily concerned with system safety engineering in the Army materiel acquisition process. Therefore, it is not discussed here. A point that should be made here is that the appropriate regulation of the Occupational Safety and Health Administration (OSHA) must be followed for Army materiel except where unique military requirements prevent compliance.

2. Nuclear safety pertaining to the nuclear warhead is unique. Although the principles of system safety for nuclear weapons are the same as those for conventional weapons, the applicable directives, standards, and specifications for nuclear weapons and equipment are a unique group of documents. Because system safety for nuclear weapons is such a highly specialized field, it is not included here.

1-4.1 DEPARTMENT OF DEFENSE DOCUMENTATION

The primary documents within the DoD relating to military system acquisition are DoD Directive 5000.1 (Ref. 7) and DoD Instruction 5000.2 (Ref. 8). DoD Directive 5000.1 provides the highest level of guidance for the acquisition of military systems. This directive does not address the requirements of system safety directly, but it does state that operational suitability of a system of which safety is a part is of equal importance to operational effectiveness.* Also it is stated in this directive that the guidance in DoD Instruction 5000.2 shall be followed. DoD Instruction 5000.2 provides uniform procedures for the direction and review of major system acquisition. Program documentation is an essential part of these procedures, and this documentation is required to contain information concerning system safety.

The key "umbrella" directive leading to the requirement for system safety programs is DoD Directive 1000.3 (Ref. 9). This directive establishes the policy that programs must be established to protect military equipment against damage or loss and DoD personnel and the general public from injury and or occupational illness.

DoD Directive 5000.36, *System Safety Engineering and Management,* (Ref. 10) is the main DoD document directly related to system safety. This document states the requirement that system safety programs be established in accordance with MIL-STD-882 (Ref. 3). The programs

_____

*See Glossary for the definitions of operational suitability and operational effectiveness.

shall start with program initiation and continue through the acquisition process of a system. Primary emphasis shall be placed on the identification, evaluation, and elimination, or control, of hazards before the production and deployment phase of a system.

1-4.2 DEPARTMENT OF THE ARMY DOCUMENTATION

The capstone document within the US Army relating to materiel acquisition is AR 70-1, *Systems Acquisition Policy and Procedures,* (Ref. 11). This regulation implements DoD Directive 5000.1, and it discusses only those policies unique to the Army. Although no system safety requirements are stated in this regulation, it endorses the system safety requirements in DoD Directive 5000.1 and DoD Instruction 5000.2.

The overall Army safety program is addressed in AR 385-10 (Ref. 1). As stated in par. 1-1.2, this regulation provides policy statements regarding the Army Safety Program.

AR 385-16 (Ref. 12) implements DoD Directive 5000.36. This regulation provides the objectives, policy, and engineering and management functions for system safety. The responsibilities of the Army staff and the major commands related to system safety also are discussed. This regulation also establishes Army system safety actions for multiple-service acquisitions.

DA Pamphlet 385-16 (Ref. 13) provides combat developers, materiel developers, testers, independent evaluators, and users with the information necessary to develop, initiate, and effectively manage a system safety program.

1-4.3 THE US ARMY MATERIEL COMMAND DOCUMENTATION

All of the previously discussed documents affect directly or indirectly the system safety activities at the Headquarters of the US Army Materiel Command (AMC). The AMC Commanding General has prepared supplements to ARs 385-10 and 385-16 (Refs. 14 and 15, respectively) to establish safety policies and assign safety responsibilities within AMC. AMC Supplement 1 to AR 385-16 establishes the system safety policies and requirements within AMC and assigns appropriate system safety responsibilities to the AMC Headquarters staff, to the major subordinate commands of AMC, to AMC program, project, or product managers, and to separate installations and activities reporting directly to HQ AMC.

1-4.4 MIL-STD-882

The previously discussed documentation addresses the general policies and requirements of system safety. These documents directly or indirectly refer the reader to MIL-STD-882, *System Safety Program Requirements,* for a detailed discussion of the technical requirements of a

system safety program. This standard is the basic document addressing in detail the requirements of a system safety program and program plan. Contractual requirements related to system safety are also addressed. The objectives of the system safety program and the system safety tasks associated with each phase of the acquisition process are presented. Detailed responsibilities of a contractor and the Government activity managing the contract are given. Other information in this standard includes general safety factors to consider during system design, a discussion of the various safety analyses that should be conducted during the acquisition process, and the criteria to be used as a guide for recommendations on the acceptance of risk.

1-5 SYSTEM SAFETY ENGINEERING AND OTHER DISCIPLINES

Most all of the disciplines involved in the design, engineering, production, and deployment of Army systems are concerned in some way with system safety. Accordingly, one of the primary functions of the system safety engineer is to integrate the safety-related planning done by various other disciplines. These other disciplines are responsible for specific categories of safety planning, but their primary responsibilities are for other services. For example, reliability engineers are concerned with the failure rates of all components in a piece of equipment, whether or not such failures are safety related.

System safety engineers have found that accidents are caused by adverse environmental effects and by errors in design, production, operations, maintenance, and disposal. Thus each technical discipline or management activity that can contribute to the elimination or minimization of these accident causes should be integrated into the system safety activities. Some of the principal technical activities that can affect the safety of a system are discussed in the subparagraphs that follow.

1-5.1 DESIGN ENGINEERING

Design engineering usually has a greater impact on system safety than does any other discipline. Design deficiencies can cause hazardous characteristics in a system, and their presence may prevent the adequate control of known hazards. Sometimes there is a domino effect, i.e., the lack of a good safety design may create other deficiencies that result in equipment failure or operator error. All of which can lead to accidents.

System designers are concerned with meeting requirements for performance, weight, size, cost, reliability, and other considerations in addition to safety. Until recently, engineering schools placed very little emphasis on educating students in safety principles and methods. Therefore, earlier graduates are not generally knowledgeable of the techniques of designing for accident prevention. At least

until very recently, the individual engineer could only acquire knowledge of safety principles and methods through experience. The amount of such experience in safety differs considerably from engineer to engineer.

Design engineers are responsible for producing safe designs, but system safety engineers must provide the safety criteria for their guidance, review the designs to insure that the criteria have been observed, and either analyze or teach designers to analyze the design for latent hazards.

1-5.2 HUMAN FACTORS ENGINEERING

Human factors engineering is concerned with optimizing the system interface with humans whenever they are in the system. Human factors engineers analyze designs to find ways to maximize error avoidance by the persons who operate, maintain, store, and transport a system. In addition to contributing hardware design features, this discipline has a role in developing safe procedures to be followed by personnel in each of the previously listed categories that will minimize the perceived need or desire to deviate from the prescribed steps.

These engineers assist in developing training programs designed to reduce human errors by teaching personnel the correct techniques for their activities and the emergency actions required to handle contingencies. In addition, studies of drawings, mock-ups, and prototypes by human factors engineers often identify deficiencies in concepts and designs. The results of such studies are recommendations for human factors engineered, safety-related changes. In their area of expertise, human factors engineers can be valuable contributors to the overall system safety program.

1-5.3 RELIABILITY ENGINEERING

Just as human factors engineers attempt to minimize human errors leading to accidents, so reliability engineers attempt to minimize equipment failures. Reliability engineers predict the effects upon the equipment and the operators that would result from failures of various components. When either the frequency or the severity of the end effects of the failure of a component would not be acceptable, the reliability engineers will recommend a change in design or an improvement in the quality of the component. In some cases complete reliability analyses of complex systems only for safety purposes have proved to be extremely costly because in some instances only a few of the many failures that could occur would result in accidents. A procedure becoming increasingly important in accident prevention is to make a reliability analysis of only those components that in the past have caused accidents when they failed or of only those components that other analyses have shown to be critical from a safety standpoint (Ref. 16).

1-5.4 MAINTAINABILITY ENGINEERING

Maintainability engineering has two interfaces with system safety engineering. The first is insuring that the hardware is designed to avoid accidents caused by equipment failure due to wear, inadequate servicing, lack of suitable replacements, or reassembly errors. The second is insuring that the design of the equipment does not endanger the operators or maintenance personnel while they are operating or maintaining the equipment.

1-5.5 MAINTENANCE ENGINEERING

After analyzing the system design, the maintainability studies, and the reliability studies, the maintenance engineer does the planning for both the scheduled and the unscheduled maintenance to be performed on the hardware. The maintenance engineering discipline contributes to system safety in three categories. First, it determines what scheduled maintenance activities must be performed, and at what intervals, to avoid hardware failures that could lead to accidents. Second, it develops the detailed procedures by which the maintenance personnel conduct the scheduled maintenance—with an objective of avoiding accidents. Third, the maintenance engineer also develops the sequences of detailed procedures to be followed by the maintenance personnel in conducting unscheduled maintenance—again, with an objective of avoiding accidents.

In general, the experienced maintenance engineering personnel—whether working within that specific discipline, as technical manual writers, or as training engineers—are highly sensitive to the requirements of system safety. They need system safety criteria, and their safety-related planning should be evaluated for maximum effectiveness. Given this guidance, they can be valuable contributors to the overall system safety program.

1-5.6 TEST ENGINEERING

Test engineering interacts closely with system safety engineering. Safety analyses conducted previously by system safety engineers will identify the hazards that will be present in any test. Therefore, test engineers can develop suitable precautionary and protective measures. Conversely, test engineering personnel can perform highly important system safety functions. They can verify whether or not specific potential hazards exist in the hardware, the procedures, or the environment; whether controls for existing hazards are adequate; and whether any unforeseen hazards are present. Failure rates and modes can be determined or confirmed by test. The adequacy of the procedures to be followed by operators or maintenance personnel can be evaluated in tests.

1-5.7 PRODUCTION ENGINEERING

With respect to the safety aspects of a design, the function of production engineering is to manufacture the product as the designer has created it. Production engineers must thoroughly plan the manufacturing process. If required, they must research and develop new tools, processes, machines, and equipment. They must also integrate the facilities and systems to produce quality products with minimum expenditures. To guide the production planning process, it is necessary for designers and system safety engineers to keep production personnel informed of safety-critical items, materials, and processes. Production engineering should make no changes in these identified areas until the changes have been analyzed by the designers or system safety engineers for potential effects.

Production personnel should be advised of safety-critical items that must be given special care because of hazards to production personnel or because a production error could eventually result in failures in the fielded equipment, which would be accompanied by accidents (Ref. 17).

1-5.8 QUALITY ENGINEERING AND CONTROL

Quality engineering and control activities are directed primarily toward the prevention or minimization of the production of defective items. Designers and system safety personnel must notify quality engineering and control organizations of items that are safety critical by means of notes on drawings or other documents so that close, appropriate inspection methods can be developed and special attention given to these items during inspection to avoid safety defects.

1-5.9 INDUSTRIAL HYGIENE

Industrial hygiene personnel are generally knowledgeable in environmental and materials problems that can produce adverse effects on personnel. They are also familiar with test equipment that can be used to determine the presence of deleterious substances. In addition, they are familiar with hazardous events and mishaps that have occurred in the field. Often they can inform a designer of the existence of hazardous problems related to his specialty and can recommend measures to eliminate or control these problems.

1-5.10 TRAINING

Much of today's sophisticated hardware must be operated and maintained in specific sequences of procedures to attain optimum results and avoid accidents. Therefore, operators and maintenance personnel must be thoroughly trained in order to minimize deviations from prescribed procedures. The curriculum of training for these personnel should include the safety features of a system or product, the significance of warnings, the demonstration of steps to be taken during contingencies, and other information necessary to minimize errors that could

result in accidents. Designers must assist training personnel in the preparation of training curricula and manuals to insure that the information passed on to trainees is accurate, uncomplicated, unambiguous, and essential.

1-6 SYSTEM SAFETY ENGINEERING AND MANAGEMENT ACTIVITIES

In addition to the different disciplines discussed in par. 1-5, there are management activities that also interface with designers and system safety engineers to advance the safety effort. Some of these management activities are discussed in the paragraphs that follow.

1-6.1 CONTRACTING

Often the components and subsystems obtained from vendors and subcontractors may fail in fielded hardware, which causes accidents. Therefore, it is necessary to insure that the items provided by vendors and subcontractors meet the same design safety criteria imposed on the prime contractor. Each contracting office should be educated to insure that items selected for purchase meet the criteria stipulated by the designer or the system safety engineer, that these requirements are included in the contract being negotiated, and that quality engineering personnel will take positive steps to insure that design safety criteria have been met.

1-6.2 BUDGETING

When budget cuts are necessary, safety or safety-related programs are often considered expendable. It is necessary that adequate funding for safety efforts be included in program estimates. Without appropriate funding support, the system safety effort is merely a futile exercise.

1-6.3 LEGAL

Federal regulations may impose specific requirements on a system to be procured by DoD. Occasionally, one of these requirements will be waived in order for the equipment to accomplish the military mission. In some cases DoD has been able to obtain exemption, such as for certain Bureau of Radiological Health requirements relating to military laser systems. When military needs appear to require exemption from a safety-related federal requirement, consultation with the Judge Advocate General may be required.

1-7 COOPERATION AND INTEGRATION FOR HIGHEST SAFETY LEVEL

Cooperation among various disciplines and activities is essential to the creation of a safe system. Exactly how this cooperation will be created and maintained depends upon the organizational structure, the interests and effectiveness, and the desires of top echelon management. If a manager with an active interest in system safety stresses that designers and other program personnel are to participate actively in producing a safe system, a safe system *will* result. However, if the manager's interest is not evident or is nonexistent, a safe system *may* result, and an unsafe system can result.

Cooperation in safety efforts will be enhanced if all of the parties concerned have a clear understanding of safety engineering concepts and objectives, if there are periodic meetings of safety working groups, and if there is joint participation in reviews to evaluate the safety problems and accomplishments during the acquisition process of a system. The effectiveness of the system safety program is directly related to the aggressive and cooperative spirit of all participants.

REFERENCES

1. AR 385-10, *The Army Safety Program*, 1 February 1979.

2. John C. Frost, "MICOM System Safety Program". Presentation to DARCOM Safety Director Conference, DARCOM Headquarters, Alexandria, VA, 1979.

3. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

4. Letter, Headquarters, US Army Armament Readiness Command, Rock Island Arsenal, IL, Subject: Impact of Current Developments on the Legal Mission of AMCGC [US Army Materiel Command, Commanding General], 7 January 1976.

5. Kmanuel Kintisch, "The Product Liability Problem", National Defense, Journal of the American Defense Preparedness Association LXV, 41-6 (August 1980).

6. Course Material for System Safety Course, AMC Field Safety Activity, Charlestown, IN, academic year 1972.

7. DoD Directive 5000.1, *Major System Acquisitions*, 12 March 1986.

8. DoD Instruction 5000.2, *Major System Acquisition Procedures*, 12 March 1986.

9. DoD Directive 1000.3, *Accident Prevention, Safety, and Occupational Health Policy for the Department of Defense*, 15 June 1976.

10. DoD Directive 5000.36, *System Safety Engineering and Management*, 6 December 1978.

11. AR 70-1, *Systems Acquisition Policy and Procedures*, 12 November 1986.

12. AR 385-16, *System Safety Engineering and Management*, 3 September 1985.

13. DA Pamphlet 385-16, *System Safety Management Guide*, 4 September 1987.

14. AMC Supplement 1 to AR 385-10, *The Army Safety Program*, 1 February 1980.

15. AMC Supplement 1 to AR 385-16, *System Safety Engineering and Management*, 3 March 1987.

16. DARCOM-P 385-23, *System Safety*, 1 June 1977.

17. MIL-STD-471, *Maintainability Demonstration*, 8 December 1978.

BIBLIOGRAPHY

Tom H. Davis, "Military Products Liability", *Trial*, 48-50 (July 1977.)

Albert Manucy, *Artillery Through the Ages*, US Government Printing Office, Washington, DC, 1949.

AMCP 706-196, Engineering Design Handbook, *Development Guide for Reliability, Part Two, Design for Reliability*, January 1976.

AMCP 706-197, Engineering Design Handbook, *Development Guide for Reliability, Part Three, Reliability Prediction*, January 1976.

AMCP 706-198, Engineering Design Handbook, *Development Guide for Reliability, Part Four, Reliability Measurement*, January 1976.

AMCP 706-200, Engineering Design Handbook, *Development Guide for Reliability, Part Six, Mathematical Appendix and Glossary*, January 1976.

AMCP 706-132, Engineering Design Handbook, *Maintenance Engineering Techniques (MET)*, June 1975.

AMCP 706-133, Engineering Design Handbook, *Maintainability Engineering Theory and Practice*, January 1976.

MIL-HDBK-472, *Maintainability Prediction*, 24 May 1966.

MIL-HDBK-727, *Design Guidance for Producibility*, 5 April 1984.

MIL-STD-470, *Maintainability Program Requirements for Systems and Equipments*, 3 January 1983.

MIL-STD-1388-1, *Logistic Support Analysis*, 11 April 1983.

CHAPTER 2
SAFETY ENGINEERING CONCEPTS AND OBJECTIVES

This chapter focuses upon the primary objective of the Army system safety program—i.e., to obtain an optimum degree of safety within the constraints of operational effectiveness, time, and cost. The system safety tasks to be performed in each of the five life cycle phases of a system are presented, followed by guidelines for system disposal. The sources and uses of safety design criteria and safety analyses to supplement those criteria are discussed. One of the main channels, the design review, for communicating system safety data is identified. Risk management, including qualitative and quantitative methods of risk assessment, is presented. The chapter concludes with examples of tradeoff studies related to the safety of weapon systems.

2-1 OBJECTIVES

The basic Army safety goal, as expressed in Army Regulation (AR) 385-10 (Ref. 1), is to minimize the loss of resources caused by preventable accidents and injuries. This goal is implemented through system safety programs that affect materiel design, procedure development, accident reporting, and training of personnel. To satisfy the goal, objectives of the system safety program have been established. The primary objectives, as stated in AR 385-16 (Ref. 2), are

1. "Maximize operational readiness and mission protection through accident prevention by ensuring that appropriate hazard control measures are designed into the system in a timely manner and at minimum cost."

2. "Ensure each safety and health risk for new designs, materiels, processes, and techniques is eliminated through design or controlled and that risks associated with residual hazards are formally accepted and documented."

3. "Minimize safety retrofit requirements."

4. "Identify hazards and manage the risk associated with these hazards for each system or facility throughout its life cycle in all possible configurations and all mission variances."

5. "Ensure that modifications to equipment or procedures and mission changes do not lessen the safety and health aspects of a system."

6. "Ensure that all systems can be demilitarized or disposed of safely."

7. "Ensure that system safety engineering and management principles are applied to developing basic technology for future systems."

Close examination of the previously stated system safety objectives indicates a fundamental system safety goal, i.e., all of the system safety activities must be undertaken in a timely, orderly, consistent, and programmed manner throughout the life of a system. These activities cannot be haphazard, inconsistent efforts undertaken as afterthoughts or only when dangers become obvious or an accident has occurred.

System safety activities also must be cost-effective. The cost of designed-in safety must be weighed against the probable savings resulting from fewer accidents.

2-2 LIFE CYCLE APPROACH TO SYSTEM SAFETY

The life cycle approach to system safety is based on the idea that accident prevention measures must be initiated as early as possible in the life of a system and carried through to the end of its useful life. It is usually much cheaper and more effective to design safety features into an item of equipment than it is to add the safety features when the item is in production or in the field. Experience indicates that some of the hazards in a newly designed system will escape detection no matter how aggressive the safety program. Therefore, the safety program for a system must remain active throughout the life of the system to insure that safety problems are recognized whenever they arise and that appropriate corrective action is taken.

In the life cycle approach to system safety, the first step is to tailor the safety program to meet the needs of the system being acquired. A major Army acquisition program will include in its system safety program almost all of the elements identified in MIL-STD-882 (Ref. 3). A small development program or a simple modification of fielded Army materiel will probably use portions of the standard. The points that follow should be considered in tailoring the safety program:

1. Mission requirements of the system
2. Size and complexity of the system
3. Quantities of the system to be fielded
4. Degree of confidence in the technologies used in the system
5. Resources available for the system safety program
6. Severity of hazards
7. Probability of the occurrence of an accident.

After the safety program is tailored to the specific system being acquired, the elements of the safety program are arranged in the proper sequence. Next these program elements are scheduled to integrate with all of the other

activities that must occur during each phase of the life cycle of the system. Following these steps will result in a system safety program that can be conducted systematically.

Associated with the life cycle approach to safety is the identification, validation, technical description, and control of critical items*—an activity that begins with the description of an operational system requirement (Ref. 4). This requires that adequate knowledge and recognition of critical items must be maintained by US Army Materiel Command (AMC) agencies from the design activity to purchasing, manufacturing, transportation, repair and/or overhaul, maintenance, and using activity.

The major elements of an effective system safety program will be examined next. Following that, each phase of the life cycle and the safety action related to each phase will be discussed.

2-2.1 SAFETY PROGRAM ACTIONS

The list of safety program actions that follows is a summary of Department of Defense (DoD) and Army requirements and inputs of practicing professional system safety engineers. The responsibilities of the various elements of the AMC for the safety program of a hardware system are covered in AMC Supplement 1 to AR 385-16 (Ref. 5) and are not restated here.

The safety program actions are

1. Establish management responsibilities for the system safety program. In addition, establish milestones of safety actions that safety managers will monitor for each phase of the life cycle of the system.

2. Brief all program personnel, if practical, on the system safety interfaces in each phase. As a minimum, provide system safety orientation briefings to those personnel not trained in safety but who have some interfaces with safety personnel.

3. Identify as early as possible the potential hazards that might exist in the proposed system as well as the potential methods for their elimination or control.

4. Specify the basic safety design criteria and the requirements to be followed for control of hazards. State the relative importance of system design features to eliminate or control hazards instead of controlling the hazards with auxiliary safety devices, warning devices, or reliance on procedures and training.

5. Evaluate the complexity and hazards of the system design from a safety viewpoint to determine whether it will be compatible with the proposed skill levels of operating and maintenance personnel in the proposed field environment.

---

*A critical item is a part, assembly, installation, or production system with one or more critical characteristics that, if not conforming to the design data or quality requirement, would result in an unsafe condition (Ref. 4).

6. Sequence the safety tasks to permit their orderly accomplishment when needed.

7. Plan and schedule tests to obtain the safety data needed for system design and to verify later the adequacy of the design safeguards.

8. Coordinate activities of the other disciplines contributing to system safety with those of the system safety personnel.

9. Verify that the designers of the system have accomplished the following specific tasks required to support the system safety program:

    a. Include safety considerations in the tradeoff studies of the alternative system design concept. (See Appendix 2A for examples of tradeoff studies.)

    b. Consult safety personnel regarding safety design criteria, potential problems, and possible solutions.

    c. Review prescribed safety criteria and insure that they are incorporated in drawings and specifications.

    d. Evaluate the system and its subsystems for hazards, and coordinate the findings with safety personnel.

    e. Identify any necessary safety devices, and, after coordination with system safety personnel, include the safety devices in the drawings and specifications.

    f. Discuss with safety personnel any information regarding incidents, malfunctions, and/or accidents obtained while monitoring tests or reviewing test reports if the information could affect system safety.

2-2.2 LIFE CYCLE PHASES AND SYSTEM SAFETY REQUIREMENTS DURING THE LIFE CYCLE

The DoD has identified five phases of the life cycle of an item of equipment:

1. Concept exploration
2. Demonstration and validation
3. Full-scale development
4. Production and deployment
5. Operating and support.

The first four phases make up another grouping referred to as the acquisition process (Ref. 6).

The number of phases of the acquisition process that are needed in the acquisition of a particular system will depend on the requirements of the system. Two or more of the phases could be combined, or possibly one or more phases could be eliminated, in a small system employing thoroughly understood, standardized technologies. Several of the phases of the acquisition process can be eliminated when a commercial item is procured by the military. Complex systems employing state-of-the-art technology normally will require all four phases of the acquisition process.

In the exercise of system safety responsibilities associated with the various life cycle phases, the responsibility for management of the total system resides within AMC agencies, which will implement policies and procedures to

assure that the objectives and requirements of Ref. 3 are met (Ref. 5). Depending upon who is responsible for performance in the various phases, the execution of the specific actions detailed for the various life cycle phases could be the responsibility of the contractor or in-house AMC activity. Ref. 7 describes the AMC participation and responsibilities. During the operating and support phase, however, the responsibility for safety liaison, monitoring, and reporting is within the AMC commands. The US Army Test and Evaluation Command (TECOM) has the responsibility for accomplishing the safety verification actions required during development testing to determine whether test items are safe for operational testing and Army use (Ref. 7).

2-2.2.1 Concept Exploration Phase

Threat projections, technological forecasts, and capability studies identify the mission need for a new or improved capability. When the need has been approved (see par. 4, Ref. 6, for information concerning approval of need), the program to satisfy this need enters the concept exploration phase. The document identifying the mission need specifies requirements that must be satisfied, but it does not describe how the requirements are to be satisfied. Hence the primary task of the concept exploration phase is to examine several ways to satisfy the need and to select the system design concept that most nearly satisfies these requirements.

A system design concept is a quick, thumbnail description of a particular system—usually a composite formed from general descriptions of all the major subsystems believed necessary for the system. For example, one system design concept for a mobile air defense weapon system might include a 25-ton tracked vehicle with turbine engine and hydromechanical transmission; armored hull; high-speed turret containing a single-barrel, 80-mm automatic cannon with a feed mechanism like that of the chain gun; feed capacity of 85 rounds of proximity-fuzed, fixed ammunition; directed by a turret-mounted, track-while-scan millimeter band radar with first-scan, lock-on capability. Another system design concept for the same weapon system might consist of a 5-ton unarmored wheeled vehicle with a high-speed reciprocating diesel engine, firing four platform-mounted, 30-mm multibarrel automatic cannon, etc.

System design concepts, or parts thereof, may come from similar systems that are operational, from developments that have been completed but not placed in operational systems, or from new developments. Occasionally, it is necessary to conduct feasibility studies to learn how new technologies can be developed to satisfy the requirement. Following the feasibility study, it may be necessary to make a breadboard model to prove the application of the new technology will satisfy the need.

When the most promising system design concepts are assembled, they must be evaluated and the best selected. The goal is to select the system design concept that will best satisfy the mission need. No system will satisfy completely all of the requirements of the mission because some of the requirements will conflict with one another. The objective is to select the design concept that satisfies as many of the needs of the mission as possible and the one that satisfies the most important need most completely. One tool that is useful in evaluating conflicting design concepts is the tradeoff study. Examples of tradeoff studies are given in Appendix 2A.

The system design concept that most nearly satisfies the mission need is selected. It may seem that concern for system safety is unnecessary during concept exploration because most of the effort is focused on concept evaluation and there is little concern for hardware development. This is not the case, however; system safety should have been a very important factor in the evaluation of each of the design concepts. Also the overall System Safety Program Plan (SSPP) should be initiated during this phase. An SSPP is a description of the planned methods to be used by a contractor or an in-house activity to implement the tailored requirements of Ref. 3, including organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration of other program engineering and management activities and related systems (Ref. 3). Specific system safety activities, from MIL-STD-882 (Ref. 3), for this phase follow:

1. "Prepare an SSPP to describe the proposed integrated system safety effort for the concept exploration phase."

2. "Evaluate all considered materials, design features, maintenance, servicing, operational concepts, and environments which will affect safety throughout the life cycle. Consider hazards which may be encountered in the ultimate disposition of the entire system, or components thereof, or of dedicated support equipment, which encompasses hazardous materials and substances."

3. "Perform a [Preliminary Hazard Analysis] PHA* to identify hazards associated with each alternative concept."

4. "Identify possible safety interface problems including problems associated with software-controlled system functions."

5. "Highlight special areas of safety consideration, such as system limitations, risks, and man-rating requirements."

6. "Review safe and successful designs of similar systems for consideration in alternative concepts."

7. "Define the system safety requirements based on past experience with similar systems."

8. "Identify safety requirements that may require a waiver during the system life cycle."

---

*PHA identifies safety-critical areas, evaluates hazards, and indicates safety design criteria to be used (Ref. 3).

9. "Identify any safety design analysis, test, demonstration and validation requirements."

10. "Document the system safety analyses, results, and recommendations for each promising alternative system concept."

11. "Prepare a summary report of the results of the system safety tasks conducted during the program initiation phase to support the decision-making process."

12. "Tailor the system safety program for the subsequent phases of the life cycle and include detailed requirements in the appropriate demonstration and validation phase contractual documents.".

2-2.2.2 Demonstration and Validation Phase

The purpose of the demonstration and validation phase is to validate the system concept selected during the concept exploration phase. To validate the concept, it may be necessary to build and test a prototype of some parts or all parts of the system. Both a development test and an operational test are conducted during this period on the prototype hardware. AMC's responsibilities—exercised by TECOM—associated with the verification of system safety are defined in par. 6h(3)ae, Ref. 5. If the system concept is demonstrated adequately by passing the tests—development and operational—the operational requirements that the system must meet to satisfy the requirement of the mission are stated in a document entitled *Required Operational Capability* (ROC). The ROC must be approved before the demonstration and validation phase is considered complete.

Since during this phase the emphasis of development of the system shifts from concept evaluation to initial hardware design, it is a very important phase for system safety. System safety should be ever present in the mind of the designer so that safety can be *designed* into the system. Also during this phase the major planning for the future system safety activities takes place. Specific system safety actions, from Ref. 3, for this phase follow:

1. "Prepare or update the SSPP to describe the proposed integrated system safety effort planned for the demonstration and validation design phase."

2. "Participate in tradeoff studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to make sure the optimum degree of safety is achieved consistent with performance and system requirements."

3. "Perform or update the PHA done during the concept exploration phase to evaluate the configuration to be tested. Prepare an [System Hazard Analysis] SHA report of the test configuration considering the planned test environment and test methods."

4. "Establish system safety requirements for system design and criteria for verifying that these requirements have been met. Identify the requirements for inclusion in the appropriate specifications."

5. "Perform detailed hazard analyses [Subsystem Hazard Analysis] (SSHA or SHA)* of the design to assess risk involved in test operation of the system hardware or software. Obtain and include risk assessment of other contractors' furnished equipment, of [Government-Furnished Equipment] GFE, and of all interfacing and ancillary equipment to be used during system demonstration tests. Identify the need for special tests to demonstrate/evaluate safety functions."

6. "Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:"

a. "Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production processes and operations."

b. "Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production."

c. "Production and manufacturing control data contain required warnings, cautions, and special safety procedures."

d. "Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity."

e. "Minimum risk is involved in accepting and using new design, materials, and production and test techniques."

7. "Establish analysis, inspection and test requirements for GFE or other contractor-furnished equipment (hardware, software, and facilities) to verify prior to use that applicable system safety requirements are satisfied."

8. "Perform operating and support hazard analyses of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or the associated risk is minimized. Identify the need for special tests to demonstrate or evaluate safety of test functions."

9. "Review training plans and programs for adequate safety considerations."

---

*SSHA identifies hazards associated with the design of a subsystem including component failure modes, critical human error inputs, and hazards resulting from functional relationships among components and equipments comprising each subsystem (Ref. 3).

SHA determines safety problem areas of the total system design including potential safety-critical human errors (Ref. 3).

10. "Review system operation and maintenance publications for adequate safety considerations, and ensure the inclusion of applicable Occupational Safety and Health Administration (OSHA) requirements."

11. "Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable US Department of Transportation (DOT), US Environmental Protection Agency (EPA), and OSHA requirements."

12. "Evaluate results of safety tests, failure analyses, and mishap investigations performed during the demonstration and validation phase. Recommend redesign or other corrective action (this paragraph does not apply to the facility concept design phase)."

13. "Make sure system safety requirements are incorporated into the system specification/design document based on updated system safety studies, analyses, and tests."

14. "Prepare a summary report of the results of the system safety tasks conducted during the demonstration and validation phase to support the decision-making process."

15. "Continue to tailor the system safety program. Prepare or update the SSPP for the full-scale...development phase and production phase.".

2-2.2.3 Full-Scale Development Phase

The objective of the full-scale development (FSD) phase is to demonstrate that the system design validated in the previous phase can go into production and that the resulting system satisfies the overall requirements of the mission. Included with the system are the principal items necessary for its production—i.e., the technical data package, operating and maintenance manuals, and repair parts. The suitability of the production prototype is determined by the conduct of additional development tests and operational tests.

Specific safety actions, from Ref. 3, for this phase follow:

1. "Prepare or update as applicable the SSPP for the full-scale development phase. Continue effective and timely implementation of the SSPP during facility final design phase."

2. "Review preliminary engineering designs to make sure safety design requirements are incorporated and hazards identified during the earlier phases are eliminated or the associated risks reduced to an acceptable level."

3. "Update system safety requirements in system specification/design documents."

4. "Perform or update the SSHA, SHA, and [Operating & Support Hazard Analysis] O&SHA* and safety studies concurrent with the design/test effort to identify design and/or operating and support hazards.

*O&SHA identifies hazards and recommends risk reduction alternatives during all phases of intended system use (Ref. 3).

Recommend any required design changes and control procedures."

5. "Perform an O&SHA for each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operations, foreseeable emergencies, disassembly, and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk controlled. Identify the need for special tests to demonstrate or verify system safety functions. Establish analyses, inspection, and test requirements for other contractors or GFE/GFP [Government-Furnished Property] (hardware, software, and facilities) to verify prior to use that applicable system safety requirements are satisfied."

6. "Participate in technical design and program reviews and present results of the SSHA, SHA and or O&SHA."

7. "Identify and evaluate the effects of storage, shelf life, packaging, transportation, handling, test, operation, and maintenance on the safety of the system and its components."

8. "Evaluate results of safety testing, other system tests, failure analyses and mishap investigations. Recommend redesign or other corrective action."

9. "Identify, evaluate, and provide safety considerations or tradeoff studies."

10. "Review appropriate engineering documentation (drawings, specifications, etc.) to make sure safety considerations have been incorporated."

11. "Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable DOT, EPA, and OSHA requirements."

12. "Verify the adequacy of safety and warning devices, life support equipment, and personal protective equipment."

13. "Identify the need for safety training and provide safety inputs to training courses."

14. "Provide system safety surveillance and support of test unit production and of planning for full-scale production and deployment. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure"

a. "Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production process and operations."

b. "Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production."

c. "Production and manufacturing control data contain required warnings, cautions, and special safety procedures."

d. "Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity."

e. "Minimum risk is involved in accepting and using new designs, materials, and production and test techniques."

15. "Make sure procedures developed for system test, maintenance, operation, and servicing provide for safe disposal of expendable hazardous materials. Consider any material or manufactured component (whether or not an identifiable spare part or replenishable component) when access to hazardous material will be required by personnel during planned servicing, teardown, or maintenance activities, or in reasonably foreseeable unplanned events resulting from workplace operations. Safety data developed in SSHAs, SHAs, and O&SHAs, and summarized in safety assessment reports must also identify any hazards which must be considered when the system, or components thereof, are eventually demilitarized and subject to disposal. (Not applicable for facilities construction.)"

16. "Prepare a summary report of the results of the system safety tasks conducted during the full-scale development phase to support the decision-making process."

17. "Tailor system safety program requirements for the production and deployment phase.".

The transition from a research and development model to a production prototype—marked by the FSD phase—is a critical one with regard to safety because engineering changes will be introduced into the original design to facilitate production. It is the responsibility of the organization responsible for safety—as emphasized by Item 14 of the previous paragraph—to be extremely vigilant to insure that engineering changes introduced into the brassboard model to facilitate production do not inadvertently compromise system safety. Occasionally, it is necessary to adapt draconian measures to emphasize this point. For example, when the 280-mm nuclear projectile was introduced into the Army inventory 30 yr ago, production engineers were denied the privilege of even changing the hinge on the warhead container without the concurrence of the development agency responsible for the safety of the projectile.

2-2.2.4 Production and Deployment Phase

During the production and deployment phase, the system is manufactured in quantity and delivered to the user or to a depot. The first few production units of the system are used for additional development tests and operational tests. The main purposes of these tests are to determine that deficiencies found by previous tests have been corrected and that the system is ready for full production and

issue to the troops. If the results of these tests are acceptable, the system enters full-scale production.

The main concerns of system safety during this phase are to insure that any additional changes introduced into the system do not adversely affect safety. These changes may be the result of deficiencies found during development tests or operational tests, value engineering considerations, or producibility considerations. Specific safety actions from Ref. 3 follow:

1. "Prepare or update the SSPP to reflect the system safety program requirements for the production and deployment phase."

2. "Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure"

a. "Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the system within the production process and operations."

b. "Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production."

c. "Production technical manuals or manufacturing procedures contain required warnings, cautions, and special procedures."

d. "Minimum risk is involved in accepting and using new designs, materials, and production and test techniques."

3. "Verify that testing and evaluation is performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity."

4. "Perform O&SHAs of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk reduced to an acceptable level."

5. "Review technical data for warnings, cautions, and special procedures identified as requirements in the O&SHA for safe operation, maintenance, servicing, storage, packaging, handling, and transportation."

6. "Perform O&SHAs of deployment operations, and review all deployment plans and procedures. Evaluate the interfaces between the system being deployed with personnel, support equipment, packaging, facilities, and the deployment environment, during transportation, storage, handling, assembly, installation, checkout, and demonstration/test operations. Make sure hazards identified by analyses are eliminated or their associated risk is

2-6

reduced to an acceptable level."

7. "Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to make sure acceptable levels of safety are kept. Identify major or critical characteristics of safety-significant items that deteriorate with age, environmental conditions, or other factors."

8. "Perform or update hazard analyses to identify any new hazards that may result from design changes. Make sure the safety implications of the changes are considered in all configuration control actions."

9. "Evaluate results of failure analyses and mishap investigations. Recommend corrective action."

10. "Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures."

11. "Conduct a safety review of proposed new operating and maintenance procedures, or changes, to make sure the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&SHAs."

12. "Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems."

13. "Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety 'lessons learned'."

14. "Evaluate the adequacy of safety and warning devices, life support equipment, and personnel protective equipment.".

2-2.2.5 Operating and Support Phase

The operating and support phase is the final phase and extends throughout the useful life of the system; it ends with the disposal of the system. During this phase, the system safety organization or person assigned the safety responsibility provides safety-related liaison to other commands and organizations having an interest in the system. The system safety organization or person works closely with the AMC Depot Command and designated system depots. The depots, aware of system performance by virtue of its supply and maintenance activities and contact with user maintenance units, discover system inadequacies that require correction to improve reliability and safety. These deficiencies are reported to the responsible commodity command and, subsequently, corrected by retrofit—the retrofit actions having been evaluated to insure that they have not introduced another hazard—at the depot or by intermediate maintenance units. The depots also assist in investigating problems and accidents involving the system and in determining corrective actions. The organization responsible for the system safety monitors these depot activities and provides support as appropriate. Specific actions performed by the depot command through the various depots are

1. Insure that the system is operated in accordance with prescribed procedures—observance of warnings and cautions—to preserve system integrity.

2. Insure that the user and AMC development activities are provided with channels of communication for reporting materiel deficiencies, safety problems, or mishaps.

3. Insure that mishaps, near-misses, and safety deficiencies are reported—after proper investigation—by the users to the system safety organization of the development activity.

4. Insure that safety reviews are conducted periodically or in response to the user's current safety problems. These reviews should seek to identify the scope of the problem, whether the problem occurs in all fielded systems, and the frequency of occurrence.

The system development organization, acting upon information provided by the depot command, should

1. Review data from the Army Sample Data Collection (SDC) Program.

2. Perform mishap analysis.

3. Prepare safety inputs to product improvement studies and/or recommendations.

4. Provide safety evaluation of fielded materiel as "lessons learned" for distribution to other materiel development organizations and depots.

5. Review safety aspects of proposed overhaul or retrofit actions.

6. Reassess and update data for safe demilitarization and disposal.

7. Monitor the updating of publications.

8. Monitor the continuation of training.

These activities continue throughout the useful life of the system. The operating and support phase contains one more safety-related activity, i.e., disposal of the system, which is described in par. 2-2.2.5.1.

2-2.2.5.1 Disposal Action

Disposal of a system or its subsystems, assemblies, or components is conducted for three principal reasons, namely,

1. Damage

2. Failure

3. Obsolescence, i.e., replaced by more combat-effective materiel.

As a result of damage or failure, individual units are subject to disposal at anytime during their useful life. However, the remaining units—usually the majority—will be disposed of at the end of the operating and support phase.

Disposal actions may involve

1. Demilitarization

2. Salvage of costly, critical, or reusable parts or materials

3. Transfer or sale to a friendly or allied nation.

One principal reason for demilitarization is to prevent access to sensitive information about the weapon system by unauthorized persons or the reuse of materiel in an unauthorized manner. Since military equipment must eventually be disposed of, consideration must be given during the acquisition process to designs that will permit safe demilitarization and disposal.

If the system is to be demilitarized or salvaged, safety and the avoidance of environmental pollution are important considerations. Systems containing explosives, chemicals, or radioactive materials compose special environmental as well as safety problems during disposal. Mechanical systems—such as energized springs, charged hydraulic units, and pressurized bottles—also present safety hazards. Systems released for commercial scrap after demilitarization, e.g., a combat vehicle, must be carefully inspected to insure that all items of explosive ordnance have been removed. In disposal actions involving destruction, a plan must be developed that can be implemented that protects personnel and the environment. The disposal of hazardous materials is a very specialized action and should not be undertaken without expert assistance.

2-2.2.5.2 Disposal Safety Considerations

Table 2-1 contains safety considerations for disposal tasks that should be accomplished—beginning in the conceptual phase and continuing throughout the life cycle phases of the system.

2-2.2.6 System Safety Life Cycle Checklist

To insure that safety is considered by the various engineering disciplines engaged in development programs, checklists are used in many engineering and operating activities. Within safety programs there are also many types of useful checklists. Table 2-2 is considered one of the most useful checklists for the safety engineer because it enables him to determine whether the safety program is organized, implemented, and progressing in a satisfactory manner. This checklist can be applied in each phase of the materiel acquisition process. Tailoring may be required to make the list apply to unusual circumstances of a particular program; this can be accomplished easily.

TABLE 2-1. DISPOSAL SAFETY CONSIDERATIONS AND TASKS

1. Establish the limits of damage or injury capability of a subsystem, assembly, or component.

2. Determine and identify the special procedures and equipment needed for handling and disposal; prepare detailed instructions for implementing the procedures.

3. Determine whether or not the material or its constituents can be safely reused.

4. Determine and identify the characteristics and amounts of hazardous material present in each item.

5. Determine the safeguards that should be employed during the disposal operations.

6. Determine current service requirements for destruction, such as Supply Bulletin 755-140-1, *Ammunition Disposition*. Insure that any procedures prescribed are in accordance with those requirements.

7. Determine whether societal impacts will occur during disposal, such as transportation through civilian communities and effects on environment.

8. Determine the availability of disposal sites for hazardous materials, e.g., radioactive waste.

TABLE 2-2. SYSTEM SAFETY PROGRAM PROGRESS CHECKLIST

1. Have designers been indoctrinated in the objectives, principles, and methods of system safety engineering?

2. Have designers been indoctrinated in the life cycle approach to system safety?

3. Are designers familiar with the safety tasks they are expected to accomplish during the current phase of the life cycle?

4. Are designers acquainted with the system safety manager or engineer who has been appointed for this program?

5. Have designers been provided with the safety criteria they will be expected to observe?

6. Are designers familiar with the types of safety analyses that they may be expected to perform or that they will be expected to assist system safety personnel in performing?

7. Are designers familiar with the need to include safety tests in overall test plans, to report any system verification problems that affect safety to system safety personnel, and the means to verify the safety of a system, its subsystems, components, and design?

8. Are considerations of system safety being included in all interdisciplinary design reviews?

9. Are safety risk assessments made early enough in the acquisition process to insure that unacceptable risks are eliminated from the system in a timely, cost-effective manner?

10. Are considerations of safety included in all feasibility, tradeoff, and other design studies?

2-3 DESIGN CRITERIA, SAFETY ANALYSES, AND SAFETY VERIFICATION

So far the discussion of the basics of system safety has been focused upon the primary objective of the Army safety program, i.e., cost-effectiveness, which is to be achieved by eliminating or controlling the hazards as early as possible in the life cycle of that system. The various phases in the life cycle of a typical system were then examined to show how system safety is applied progressively and cost effectively. The basic tools—safety design criteria, safety analyses, and safety verification—of the safety engineer now will be presented.

This paragraph addresses four main questions, i.e.,

1. Where do safety design criteria originate?

2. What role does safety engineering play in disseminating these criteria?

3. Given the existence of these criteria, why perform safety analyses?

4. How can the safety engineer verify the safe design of a system?

Whether the Army safety engineer is working with an Army program in-house or is supporting the program or project contracted for, he must be familiar with the applicable safety design criteria. These criteria arise from many sources. A likely starting point is the historical safety information on predecessor systems and the application of lessons learned. Historical safety information is available from the following sources (Ref. 8):

1. The US Army Safety Center (USASC) maintains a computerized data base, the Army Safety Management Information System (ASMIS), containing accident information. Safety lessons learned are also available. Information can be obtained from USASC, ATTN: PESC-D, Fort Rucker, AL 36362-5363.

2. The US Army Human Engineering Laboratory (HEL) develops lessons learned in the area of human factors. Information can be obtained from HEL, ATTN: AMXHE-DA, Aberdeen Proving Ground, MD 21005-5001.

3. The US Army Materiel Readiness Support Activity (MRSA) maintains the maintenance data base, integrated logistic support (ILS) lessons learned, and has recently established the Manpower and Personnel Integration (MANPRINT) data base. Also, MRSA is in the process of developing a health hazard assessment data base. Information can be obtained from MRSA, ATTN: AMXMD-EI, Lexington, KY 40511-5105.

4. The Air Force maintains a lessons learned data base. All lessons learned, including safety, are consolidated at the Air Force Acquisition Logistics Center (AFALC) by the Directorate of Lessons Learned. Information can be obtained from AFALC, AFALC/PTL, Wright-Patterson AFB, OH 45433.

5. The Navy maintains computerized safety lessons learned and accident data. Information can be obtained from the Naval Safety Center, Code 90, Naval Air Station, Norfolk, VA 23511.

6. The US Army Materiel Systems Analysis Activity (AMSAA) prepares liaison activity reports that compile safety-related and other data regarding user perceptions on the effectiveness of fielded systems. Information can be obtained from AMSAA, ATTN: AMXSY-L, Aberdeen Proving Ground, MD 21005-5071.

7. The materiel proponent maintains safety-of-flight, safety-of-use, equipment improvement, and quality deficiency reports. (See AR 95-18 (Ref. 9), AR 750-10 (Ref. 10), DA PAM 738-750 (Ref. 11), and DA PAM 738-751 (Ref. 12).) A Quality Deficiency Report (QDR)—prepared by anyone in the Army who identifies a quality defect in a specific Army item—can be obtained from the Quality Assurance Directorate of the appropriate Army command. An Equipment Improvement Report (EIR) offers a suggested change to improve the design of an item of Army materiel. EIRs are stored at the responsible commodity command; copies may be obtained by written request. Additional information on QDRs and EIRs can be obtained from DA PAM 385-16 (Ref. 13) and DA PAM 738-751 (Ref. 12).

8. The Defense Technical Information Center (DTIC) can provide information on research being planned, research currently being performed, and results of completed research. Information can be obtained from DTIC, ATTN: DTIC-DDR-1, Cameron Station, Alexandria, VA 22314.

9. Users of predecessor systems maintain historical safety information. User safety offices at major Army commands can provide system safety input.

Additional sources of safety data are specifications and standards for specific types of materiel that are sponsored by the Army, DoD, other Government agencies, and private professional groups such as the American National Standards Institute (ANSI) and the Society of Automotive Engineers (SAE). Civil codes are appropriate sources of safety critieria if the new materiel will be developed, tested, or operated in areas that are under the control of a civil authority. Commercial safety criteria are applicable for commercial items, e.g., passenger vehicles and trucks, which are introduced directly into the Army inventory.

2-3.1 THE NATURE OF SAFETY DESIGN CRITERIA

Safety criteria are often confused with safety requirements. The distinguishing characteristic is simply that safety criteria are broad in coverage and that safety requirements are more detailed. For example, safety criteria may require that the hardware be designed such that a specific unwanted event cannot occur unless three

independent failures take place. The comparable safety requirement may state that the same unwanted event cannot occur unless three specific switches fail in a specific sequence and manner.

Safety guidance may be conveyed by safety criteria as a performance objective or as a specified safety requirement. The performance objective establishes the desired end result; it specifies how the system will perform but not the specific means by which the objective is obtained. The designer is permitted to select the means of achieving the objective through the choice of design, dimensions, materials, and other considerations. On the other hand, a specified safety requirement dictates the exact design; length, width, and height; construction; finish; and other detail concerning the object. Most designers prefer the performance objective because it is less restrictive, but specified requirements can be beneficial. For example, a specified safety requirement may state that the opening in a guard to protect the fingers of an operator will be no greater than a specified dimension. Thus the designer does not have to research and establish anew the correct size of the opening as he would if given a performance objective such as, "The opening will not be large enough to permit the operator's finger to enter the danger zone.".

Not every existing military specification or standard covers all aspects of design neatly for a given category of equipment. An exception is MIL-STD-454 (Ref. 8), which contains safety requirements applicable to all electrical and electronic systems developed for the Army and other DoD agencies. There is no similar document, however, that applies to all pressure systems, for example. In such a case, safety criteria and requirements applicable to a particular acquisition program must be compiled from a group of documents related to various aspects and components of the pressure system. Unfortunately, the multiplicity of safety data derived from various kinds of standards and specifications, codes, books of rules, and manuals may make the designer's task of selecting the applicable criteria or specification difficult. In these instances the safety engineer can assist the design engineer in making the proper choice.

Certain safety criteria and requirements appear to be so fundamental that they are referred to as "good engineering practices". Unfortunately, new design engineers spend many years learning these fundamental practices, and, often by the time the designers have acquired these skills, the engineers have been promoted to positions that may be more administrative than technical. Consequently, the safety engineer should be encouraged to record and publish these "good engineering practices" in the form of specific safety requirements.

The safety engineer should not perfunctorily distribute safety data to designers; the safety engineer should do his homework first, i.e., consider the effect that various safety criteria and specifications will have on the system. Even

when safety criteria and specifications are applied to a system conscientiously, unsafe conditions—which can only be revealed by analyses, studies, and tests—may still be present in the system. For example, a requirement in an electrical standard stipulates that a red button will be provided to shut off power to the equipment in an emergency. Questions arise, however, that can only be answered by analysis or test, which must be performed before incorporating the safety device. Example questions that require answers are

1. What conditions constitute an emergency?

2. Can the need for the emergency circuit be eliminated?

3. Can design action be taken to prevent an emergency?

4. Can a person involved in an emergency situation reach and use the red button if it is incorporated?

5. What will be the consequences of pushing the red button and shutting off the power?

6. Will the emergency system react fast enough to avoid and minimize injury or damage?

7. Do tests verify that the emergency system will operate as required?

A good rule to follow is to perform a safety analysis before applying a proposed safety criterion or requirement to verify that it will provide the desired safety effect. Accordingly, safety analyses must supplement the use of safety-imposed directions. In some cases, directly applicable analyses exist for related systems and are available through the Army SDC program. In this case, the only necessary action required by the safety engineer is to verify that the applicable safety information is distributed and used as appropriate. For example, certain electrical hazards are so well-known from accident investigations and analyses that preventive measures have been developed as safety requirements—i.e., electrical insulation, bonding, or grounding. The designer does not have to consider how to implement a safety criterion to eliminate an electrical hazard; he simply applies the requirements already developed. The adequacy of the insulation used, however, may require verification by test.

In summary, early in the system development program, the safety engineer assembles applicable safety design data from a wide variety of sources. As required, he then distributes the information to design engineers involved in the program. When questions arise, he interprets the safety criteria and lists them according to priority. For his own use the safety engineer evaluates the probable effects of the various safety criteria and requirements on the system being designed. He identifies those system data items that might produce questionable or marginal effects or will enhance system safety, conducts safety analyses of those applications, and conveys the results to the designers. The other major activity performed by the safety engineer is to verify the safety of the system. Safety verification is described in par. 2-3.2.

2-10

2-3.2 METHODS OF PROOF OF SAFETY

Safety demands having been designed into a system, the safety must be verified with proof that the system or any of its subsystems or components has or does not have specific properties, will or will not behave in a given manner, and can or cannot perform specific operations. Verification may be accomplished through four different methods, or combination of these methods, as follows:

1. *Analysis.* A proof-of-design analysis consists of analyzing the original engineering calculations to determine whether the design hardware will maintain its integrity when performing as required. Loads and stresses, and the dimensions of different materials to provide these strengths; and acceleration, velocity, and reaction time are checked. Other engineering calculations made by design engineers to insure their designs adequately provide for the safe performance of the proposed equipment are verified. Examples include the analysis of the thickness of a specified metal for a pressure vessel or the specification of the number and size of bolts to join two parts of an equipment frame together. Although used for safety purposes, the proof-of-design analysis is not considered a safety analysis in the sense of those analyses included in Chapter 3.

2. *Examination or Inspection.* This type of verification consists of personal observation to determine whether a specific adverse condition exists or to identify evidence of workmanship or the presence of an unsuitable or proscribed material. The process includes gaging or measuring to insure compliance with requirements and inspecting for the presence of required safety devices. Generally, verification by examination is accomplished without the use of special laboratory equipment or procedures. Examples of conditions typically verified by examination are the presence of mechanical hazards that can cause injury to human appendages or flesh, electrical circuits open to human contact, and warning labels and the determination of whether the dimensions of the openings in a guard are appropriate.

3. *Demonstrations.* Demonstrations are conducted to show that safe operations can be achieved as claimed and specified. Demonstrations usually involve a "go" or "no go" situation, i.e., that a piece of equipment will operate in a safe, desirable manner and not in an unsafe, undesirable manner or that a material has or lacks a certain property. Examples of situations suitable for the demonstration method include the demonstration that the use of an emergency button will halt the operation of a piece of equipment or the demonstration that a fabric or insulation is either nonflammable or self-extinguishing.

4. *Tests.* Tests are a means of verification in which devices are used to measure specific parameters. Tests are conducted to determine whether the measured results do or do not fall within the required or acceptable limits. Conversely, tests can also reveal that the application of a specified load, stress, or other condition will not cause failure, damage, or a hazardous condition. Examples include proof-or-burst tests on pressure vessels, tests of equipment sound levels, and tests of bolt strength.

2-4 SAFETY DESIGN REVIEWS

The safety engineer coordinates frequently and informally with design engineers, human factors engineers, and other program team members; but the forum in which he presents the results of his work, and in turn is formally apprised of programs and problems, is the design review. Because the review is so important to the safety engineer as a principal channel of communication, the two reviews likely to be encountered are described, i.e.,

1. *Interdisciplinary Design Review.* This is a review and evaluation of the design that was conceived, proposed, or created in the materiel acquisition process. It is not a safety design review as such, but each of the elements covered will have a safety connotation.

2. *Specific Safety Review.* This review is performed specifically to evaluate the safety features of a system and its subsystems.

These reviews are discussed in pars. 2-4.1 and 2-4.2, respectively.

2-4.1 INTERDISCIPLINARY DESIGN REVIEW

This type of review is a general review, or milestone, at which the progress in design, development, test, or production of a system or subsystem can be evaluated by all concerned. Common examples are Preliminary Design Reviews (PDRs) and Critical Design Reviews (CDRs). These design reviews may be conducted at the direction of any level of management for in-house or contracted programs. A program manager, company manager, or acquisition activity commander can hold a review to evaluate an entire program to decide whether it should continue as is or whether it requires changes, corrections, or additional efforts. Similarly, a supervisor responsible for the design of a unit or subsystem may hold reviews to determine progress, direction, and details of the unit or subsystem design.

Information usually presented at such design reviews will cover the goals to be achieved, the methods used for their accomplishment, the progress made, and the problems encountered. Frequently, the action recommended in a design review is based on a consideration of safety. Before a specific action is recommended or adopted, a documented tradeoff study should be prepared. (See examples of tradeoff study results under par. 2-5, "Risk Management".) It is good practice for designers making tradeoff studies to include the system safety engineer in the decision process to provide expertise in determining

and evaluating potential hazards, risk assessments, and possible preventive or corrective measures.

The analyses given by a system safety engineer in a design review may include the probable location of hazards, methods used to eliminate or control the hazards, or assurance that specific hazards will not be present. Designers at the review may respond with options for hazard control, the salient features of each option, and recommended action.

2-4.2 SPECIFIC SAFETY REVIEW

These reviews are devoted specifically to evaluations of the safety features of a system. The review might encompass the entire system, a subsystem or component, or a specific safety feature of the system. Reviews may be undertaken at the request of an outside safety organization, or they may be requested or required by the program manager at a specific milestone in the program, or they may be convened by the system safety organization of the program. For example, the system safety organization may request that a board experienced in explosive safety matters review the types, effects, and safeguards that might be present in any new system and determine whether all restrictions on such explosives have been or will be met. The board could be an existing one, such as the AMC Fuze Board to insure that the provisions of MIL-STD-1316 (Ref. 14) have been met or an *ad hoc* board convened to examine a specific feature.

Army acquisition activities also may convene reviews with system safety working (*ad hoc*) group members from their staffs, the intended users, the probable logistic support activity, and command safety agencies. In these meetings either the organization developing the system or a test activity presents safety-related information about the entire system or any of its aspects. The group recommends to the program manager that the acquisition process is to proceed, or it may direct changes or additional effort.

Within a contractor organization the internal system safety review group is sometimes designated by other titles, but it serves a similar function. Usually the system safety working group is a committee—reporting to a higher management level—of representatives from development, test, production, quality control, and other organizations. The working group allocates specific safety tasks, resolves problems, and reviews solutions to problems encountered in the conduct of the safety review of the system.

2-5 RISK MANAGEMENT

According to MIL-STD-882 (Ref. 3), risk is defined as "an expression of possibility of a mishap in terms of hazard severity and hazard probability". The objective of system safety is to eliminate hazards when possible and control them when elimination is not possible—consistent with mission requirements and cost-effectiveness. The safety engineer, however, cannot accomplish this alone. His job is to make recommendations, backed by sound research and analysis data, to the program management team. The program management team weighs the safety engineer's data and outside factors to arrive at informed decisions regarding changes in the system to optimize safety. The process by which the safety engineer gathers his data and generates his recommendations is called risk management.

In the paragraphs that follow, the steps involved in risk management are investigated. As a first step, the safety engineer analyzes each facet in the planned use of the new system and identifies the potential hazards. Next he analyzes the risk represented by each hazard. Two major methods—quantitative and qualitative—are used to assess risks. As the final step, the safety engineer recommends that the risk be eliminated, controlled, or accepted.

2-5.1 HAZARD IDENTIFICATION— NECESSARY FIRST STEP

To make risk assessments of the hazards in any system, those hazards must be known. Therefore, hazard identification must be the initial step in any risk management program. (Methods of analysis used to identify hazards are described in detail in Part Two of this handbook.) Each particular mode of system operation must be analyzed to identify the hazards associated with it. For example, some hazards that are encountered in mission operation may not apply to maintenance operations and vice versa. Even in a particular mode of operation there can be separate operating elements—e.g., refueling of combat vehicles during battle—that require individual analysis. In each case, only the hazards present in that particular element are considered in risk assessment. After the hazards have been identified, the represented risks must be assessed. Of the two major methods for assessing risk, the quantitative methods (par. 2-5.2) are discussed first.

2-5.2 QUANTITATIVE RISK ASSESSMENT METHODS

Numerous quantitative risk assessment methods have been in use for a long time. Many were developed for specific purposes and have met with varying degrees of success. The examples to be discussed are probabilities of occurrence, toxicology quantification, relative numerical ratings, and safety factors and margins.

2-5.2.1 Probabilities of Occurrence

The calculation of the probabilities of part failure rates to support reliability predictions of new materiel in the acquisition process are also useful for safety analyses and risk assessments. To understand more about the strengths and weaknesses of probability forecasting, the use of probabilities in other industries is examined.

Probabilities are used as the basis for risk acceptance and rate setting in much of the insurance industry. For example, life insurance is based on experience data derived from mortality statistics. However, even with life insurance, for which ample data have been accumulated over a long time for large populations, the predictions must be updated periodically if they are to be used with confidence. Although the life insurance industry can make reasonably accurate predictions over the long term, its predictions for the short term or for individuals are often in error. The National Safety Council, basing its predictions on past data with foreseeable adjustments, will predict that during a given holiday there probably will be a certain number of accidents and a specific number of persons killed. However, a change such as a sudden onset of bad weather, or an increase in the price of gasoline, or a popular sports event shown on television during that holiday may reduce the actual number of accidents and deaths far below that predicted. Even though accident statistics provide a large data base, circumstances do affect the short-term accident predictions. Circumstances also will affect prediction in Army materiel acquisition programs.

Far less reliable than traffic accident and mortality predictions are the predictions of occurrences of low probability events such as airplane crashes, train wrecks, and explosions of chemical plants. Not only are the forecasters hampered by a smaller number of statistics but also they have great difficulty finding comparable circumstances because an accident caused by equipment failure generally leads to corrective actions, which changes the original conditions and circumstances. This invalidates the previous experience data. An example of unrelated data is that pertaining to accidental fires in Army tanks previously fueled with gasoline when diesel engines were introduced. These data for gasoline fuel, however, were not valid for accident predictions involving diesel fuel because the conditions were not the same.

Recognizing that a new system may not have the same conditions as fielded equipment and that the exact conditions for the new system may not be definable until the program is well along, MIL-STD-882 (Ref. 3) states in par. 5.4.3.2, "Assigning a quantitative hazard is generally not possible early in the design process.".

In spite of these limitations, probabilistic methods of risk assessment are still being employed—e.g., in predictions of failure rates and by assignments of probabilities to occurrence of specific failures.

2-5.2.2 Toxicology Quantification

Ref. 15 attributes this statement to Paracelsus (1493-1541): "All things are poisons, for there is nothing without poisonous qualities. It is only the dose which makes the thing a poison.". For risk assessments involving the toxic effects of hazardous materials, it has been proven that the dosage or amount of the chemical required to produce harm is the most important factor. The hazard is the probability that injury will be caused by the circumstances of the exposure (Ref. 15).

Toxicity can be subdivided on the basis of
1. Duration of exposure from short- to long-term
2. Site of action of the toxic agent at point of contact or by absorption.

To establish the conditions for accurate risk assessment of toxicity at least six other factors should be considered (Ref. 15), i.e.,
1. Route of exposure
2. Type of formulation or state of dispersion of toxicant
3. Temperature
4. Humidity
5. Physiologic condition of suspect
6. Interaction of toxicant with other chemicals or drugs.

To understand the numbers and notations associated with toxicity risk assessments, several examples are presented. LD_{50} is the term commonly used to present a statistical estimate of the dosage necessary to kill 50% of an infinite population of test animals. ED_{50} is the dosage necessary to produce a particular effect in 50% of an infinite population of test animals. In these examples, the L stands for lethal, E for effective, and D for dose; the 50 represents percent affected.

For industrial and occupational exposure restrictions to airborne concentrations, the notation TLV (Threshold Limit Value)—formerly known as Maximum Allowable Concentration (MAC)—is used. Although LD_{50} and ED_{50} are experimentally derived, the TLVs are arbitrarily set on the basis of the best data available. The TLV number represents the maximum concentration of airborne material—i.e., dusts, fumes, mists, vapors, or gases—to which workers may be exposed. Under specified conditions no significant harm is expected if the worker is exposed to the TLV environment eight hours a day for five days a week.

It is evident that toxicological risk assessment is highly specialized. Prior to attempting such a risk assessment, the safety engineer should consult the appropriate section of Ref. 15 (or the equivalent). Also the results of the assessment and the supporting analysis should be checked by a specialist in this field.

2-5.2.3 Relative Numerical Ratings

Another quantitative method of assessing risk is to assign numerical indicators to hazards in order to compare them with one another. Various systems of numbers—e.g., 1 through 4, 1 through 6, 1 through 10—can be used to compare particular characteristics of the items under study. These values will be relative and based on a numerical scale that generally has no significance except for comparative purposes. The comparisons, however, will be useful only if the meaning of each number in the scale has been defined.

In certain cases the relative numerical rating system can be quite useful. For example, a material, such as a liquid, might have three potential hazards associated with three separate characteristics of the liquid. It might have toxicity, flammability, and corrosiveness characteristics. Each of these hazards can be compared with the characteristics of other liquids, and the liquids can be compared overall by assigning each physical characteristic a numerical rating system and a separate system to the liquid itself to indicate its relative desirability or undesirability. The latter system could be simply a sum of the scores of the three characteristics of the system, or it could be a more sophisticated weighted system. The weakness of relative numer-

ical ratings is that they are dependent on the raters who interpret the definitions, make judgments, and assign the numerical values. Thus it is important that when a numerical system is to be used, the definition of each number be made as specific and clear as possible. Commonly used numerical rating systems, e.g., 1 to 10, are better understood by large numbers of personnel and generally yield more uniform results.

2-5.2.4 Safety Factors and Safety Margins

Safety factors are another quantitative method of risk assessment. They initially were established for use with structures and are based on the concept that an item should be overdesigned to compensate for material strength variances, overloads, manufacturing variances, or fatigue. Theoretically, a component designed with a safety factor of 4 should be twice as strong as one with a safety factor of 2. In many cases this theory is not true because production or material differences in large lots cause actual strengths to differ. Two items from the same production run are designed to the same safety factor, but manufacturing variances will produce variances in their individual safety factors, and this complicates the assessment of risk based on the theoretical safety factor. Good quality control in the manufacturing process is essential to establish confidence that each item produced will exhibit the designed-in safety factor. In effect, safety factors are also used in electronic system design; the term for this application is "derating". Thus if a manufacturer needs an electronic component that will carry a specific load, he will select a component that can carry a much higher load.

Safety margins are another quantitative method of risk assessment. A safety margin is the ratio of the difference between the lowest limit in a statistical strength distribution and the highest stress divided by the lowest limit strength. This system can be applied to many variations of mechanical designs. The statement is represented by the equation

$$\text{safety margin} = \frac{\text{strength (min)} - \text{stress(max)}}{\text{strength (min)}} \quad (2\text{-}1)$$

In observing representative methods of quantitative risk assessment, it can be seen that each method has advantages, disadvantages, and specific applications. Qualitative methods are discussed in par. 2-5.3.

2-5.3 QUALITATIVE RISK ASSESSMENT METHODS

The prescribed method in MIL-STD-882 (Ref. 3) for making risk assessment by qualitative means involves two factors. First, hazard severity categories indicate the potential adverse consequences that can result from personnel error; environmental conditions; design inadequacies; procedural deficiencies; and system, subsystem, or

component failure or malfunction. These hazard severity categories range from I (catastrophic) to IV (negligible). Second, there are five qualitative levels to represent the probability of the occurrence of a hazardous event, which range from A (frequent) to E (improbable). The definitions of severity categories and qualitative levels are shown in Tables 2-3 and 2-4, respectively. This method takes both factors into account for risk assessment, as shown in Table 2-5.

TABLE 2-3. DEFINITION OF HAZARD SEVERITY CATEGORIES (Ref. 3)

Description	Category	Mishap Definition
Catastrophic	I	Death or system loss
Critical	II	Severe injury, severe occupational illness, or major system damage
Marginal	III	Minor injury, minor occupational illness, or minor system damage
Negligible	IV	Less than minor injury, occupational illness, or system damage

TABLE 2-4. DEFINITION OF QUALITATIVE LEVELS OF HAZARD OCCURRENCE (Ref. 3)

Description	Level	Specific Individual Item
Frequently	A	Likely to occur frequently
Probable	B	Will occur several times in life of an item
Occasional	C	Likely to occur sometime in life of an item
Remote	D	Unlikely, but possible, to occur in life of an item
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced

TABLE 2-5. CLASSIFICATION OF SAFETY DEFICIENCIES AND SHORTCOMINGS

Severity Category		Hazard Probability				
		Frequent A	Reasonably Probable B	Occasional C	Remote D	Improbable E
I	Catastrophic	Deficiency	Deficiency	Deficiency	Deficiency	Suggested Improvement (Acceptable)
II	Critical	Deficiency	Deficiency	Deficiency	Shortcoming	Suggested Improvement (Acceptable)
III	Marginal	Deficiency	Shortcoming	Shortcoming	Suggested Improvement	Suggested Improvement (Acceptable)
IV	Negligible	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

The most common illustration of the qualitative method of risk assessment would be a hazardous event caused by part failure. The severity of the event can be evaluated and a hazard severity category applied from the definitions in Table 2-3. The assigned probability of occurrence from Table 2-4 will be related to reliability data obtained from tests, tables of applicable data, or estimation. The classification level will be established by qualitatively matching the probability with the severity level in Table 2-5. It may be more difficult to assign a probability level to hazardous events caused by other than parts failures; in these cases the safety engineer examines all types of experience data to find valid relationships.

The qualitative method of risk assessment is useful as a guide—when the categories and qualitative probability levels are available for decision making as to whether corrective actions are warranted—as shown in Table 2-5. The decision limit moves up the scales and from the left—from Category III with frequent probability to Category I with remote probability. Any situation of lesser severity or probability than these values will fall into "shortcoming", "suggested improvement", or "acceptable". In all cases where a quantitative analysis is to be performed for whatever reason, it should be first structured through the use of a qualitative safety analysis.

Since the method illustrated in Table 2-5 is only a method of guiding management personnel, a decision involving a safety "fix", or improvement in design for safety where high cost is involved, may require other types of supporting safety analyses. Emphasis is appropriate at this point regarding the safety program objectives that remain firm throughout all discussion areas. All hazards should be eliminated or minimized if possible and controlled when not possible, consistent with the requirements of the mission and cost-effectiveness.

2-5.4 RISK ACCEPTANCE

The degree to which hazards in a system can be eliminated or controlled is greatly dependent upon the capabilities of the designers. Experienced system safety engineers, however, can assist the designers by evaluating more effectively the possible safer alternatives. The system safety program is designed to provide a disciplined approach not only to identify hazards but also to effect their elimination or control. Whether the risks of accidents caused by these identified hazards are acceptable will determine whether or not action will be taken to eliminate or control a hazard.

Army attitudes toward risk acceptance have changed in recent years. In the past it was believed that military equipment need not be as safe as that for civilian application since the military profession is a comparatively high-risk occupation, especially when a person is serving in a combat unit. Thus the level of acceptable risk could theoretically be much higher for military personnel than for civilians. Now, however, commands increasingly recognize that the consequences of accidental loss of a military system or of military personnel may be devastating to operational accomplishment. Acceptable risk levels may, as a result, have to be as low as E or lower than for civilians.

In the 1960s and 1970s manufacturers and operators of military equipment informally established and used a standardized number to represent acceptable risk levels in all cases. This number, 10^{-6}, represented the risk level of 1 out of one million operations that might result in a failure that would cause an accident. However, there are too many variables in assessing acceptable risks for one standardized number to be useful under all circumstances. In each case the specific circumstances and

exceptions to the general circumstances must be considered carefully.

Defining risk acceptance by rigid rules is very difficult. In practice it has been found wise to make risk assessments considering all the factors involved in each case. Severity and probability of occurrence are only two of the factors to be considered in making management decisions. Additional factors are cost, program time involved, technology, material and parts availability, and performance. Whether or not any level of risk is acceptable must be determined by the specific circumstances and consequences of potentially hazardous events. In some instances the benefits derived from a design or material that can generate severe adverse consequences if a failure occurs may outweigh the disadvantages. The decision to assure immediate acquisitions of large ballistic missile systems led to the acceptance of the hazards involved with the use of liquid propellants. Later, when the immediate need was overcome, acquisition of far less hazardous systems using solid propellants made the use of liquid propellants unacceptable. In other instances it may be decided that risks can be reduced at little or no cost or delay. Then the use of the proposed design change or other program action to reduce hazards is highly desirable.

Improvements requiring costly design effort or parts, delays in the program, degradation of performance, or procedures limiting combat effectiveness are not easy decisions to make. Each of these actions may require separate analysis and study with inputs from combat developer as well as the development, testing, training, and depot commands.

The task of weighing all of the factors involved in making changes to the system in order to eliminate or control a hazard and in deciding whether or not to make those changes lies ultimately with program management. It is the job of the safety engineer to identify each hazard, analyze it, assess its risk, and make recommendations to management regarding its disposition. The skill with which he does his job will play a significant role in the decisions that are made.

REFERENCES

1. AR 385-10, *The Army Safety Program*, 1 February 1979.

2. AR 385-16, *System Safety Engineering and Management*, 3 September 1985.

3. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

4. AMC-R 702-32, *Critical Safety Item Program*, 28 January 1986.

5. AMC Supplement 1 to AR 385-16, *System Safety Engineering and Management*, 3 March 1987.

6. DoD Directive No. 5000.1, *Major System Acquisition*, 12 March 1986.

7. DARCOM-P 385-23, *System Safety*, 1 June 1977.

8. MIL-STD-454, *Standard General Requirement for Electronic Equipment*, 1 March 1985.

9. AR 95-18, *Safety-of-Flight Messages*, 12 July 1985.

10. AR 750-10, *Modification of Materiel and Issuing Safety-of-Use Messages and Commercial Vehicle Safety Recall Campaign Directive*, 1 December 1982.

11. DA Pamphlet 738-750, *The Army Maintenance Management System (TAMMS)*, 1 December 1983.

12. DA Pamphlet 738-751, *Functional Users Manual for the Army Maintenance Management System, Aviation (TAMMS-A)*, 28 June 1985.

13. DA Pamphlet 385-16, *System Safety Management Guide*, 4 September 1987.

14. MIL-STD-1316, *Fuze, Design Safety, Criteria for*, 3 January 1984.

15. Irving Sax, *Dangerous Properties of Industrial Materials*, Fourth Edition, Van Nostrand Reinhold Company, New York, NY, 1975.

BIBLIOGRAPHY

K. A. Pullen, *The Design of Communication Systems*, RN 1186, Ballistic Research Laboratories, Aberdeen Proving Ground, MD, December 1962.

AIR-290-60-FR-225, *Human Factors Methods for System Design*, American Institute for Research 410 Amberson Avenue, Pittsburgh, PA, 1960.

Cyril M. Harris, *Handbook of Noise Control*, McGraw-Hill Book Co., Inc., New York, NY, 1957.

A. D. Swain, *Safety as a Design Feature in Systems*, SCR-65-991, Sandia Corp., Albuquerque, NM, September 1965.

Sliney and Wolbarsht, *Safety With Lasers and Other Optical Sources*, Plenum Press, New York, NY, 1980.

APPENDIX 2A
EXAMPLES OF SAFETY TRADEOFF STUDIES

These examples illustrate the factors typically considered by the Army in tradeoff studies. They are based on discussions with manufacturers and Army personnel and on the author's experiences.

2A-1 ADVANCED ATTACK HELICOPTER FUEL TANKS

2A-1.1 PROBLEM AND ANALYSIS

The problem was whether to use self-sealing fuel tanks or the conventional aluminum tanks in the AH64A helicopter. The analysis of this problem is presented in Table 2A-1.

2A-1.2 ALTERNATIVE TO SELF-SEALING TANK

A conventional aluminum tank filled with a plastic, spongelike foam will provide protection against major splashing of fuel in an accident. A broken fuel tank will allow fuel to escape and burn, but the fire will be somewhat reduced. Holes in the tank from enemy fire will allow leaks, but the fuel will not escape as fast as it would without the foam. An aluminum tank with the foam is lighter in weight than a self-sealing tank, and it is not quite as expensive. This tank can carry slightly more fuel than the same size self-sealing tank.

2A-1.3 CONCLUSION

The positive factors in this tradeoff analysis providing safety and performance advantages outweighed the disadvantages, and the self-sealing tank was adopted for the AH64A helicopter. The alternative was not judged to offer sufficient advantages or to reduce the disadvantages sufficiently to justify its use over the self-sealing tank.

2A-2 ADVANCED ATTACK HELICOPTER ENGINES

2A-2.1 PROBLEM AND ANALYSIS

The problem was whether to use one or two engines in the AH64A helicopter. The analysis of this problem is presented in Table 2A-2.

2A-2.2 ALTERNATIVE TO TWO ENGINES

There is no alternative to gaining two-engine capability with fewer than two engines. A single engine can be designed to drive a two-rotor helicopter, but it will still be subject to the disadvantages of single-engine failure.

2A-2.3 CONCLUSION

In this tradeoff analysis the advantages of safety and performance outweighed the disadvantages, and the two-engine installation was selected for the AH64A helicopter.

2A-3 LIGHTING FOR GROUND VEHICLES USED IN COMBAT ZONE

TABLE 2A-1. SELF-SEALING TANKS VS CONVENTIONAL ALUMINUM TANKS FOR THE AH64A HELICOPTER

Advantages of Self-Sealing Fuel Tanks	Disadvantages of Self-Sealing Fuel Tanks
1. Accidents that would be survivable except for the spilled fuel and resulting fire will be survivable.	1. Self-sealing tanks cost more than conventional tanks.
2. Enemy fire into fuel tanks will be less effective in downing a helicopter.	2. Reduction in volume of fuel that can be carried and, therefore, reduction in mission time and range.
3. Minor leaks in a conventional tank, which would cause mission delay for repairs, will be eliminated.	3. Reduction in payload (ammunition) that can be carried because of the increase in tank weight.
	4. Possible loss of self-sealing capability over long periods, which would require replacement of self-sealing tank.

TABLE 2A-2. TWO ENGINES VS ONE ENGINE FOR THE AH64A HELICOPTER

Advantages of Two Engines	Disadvantages of Two Engines
1. Autorotation landings after single-engine failure, with consequent high accident rate, are eliminated. 2. Mission can be completed on single engine in all situations except those requiring maximum performance. 3. Forced landing in enemy territory because of single failure will be prevented. 4. Mission equipment, including essential flight instruments, has an alternate power source. 5. The engines and their parts are smaller, of less weight, and can be handled more easily.	1. Two complete engines and installations cost more. 2. Total engine weight of a two-engine installation is greater. 3. Maintenance time is increased for two engines and installations. 4. Number of repair parts is higher with two engines.

2A-3.1 PROBLEM AND ANALYSIS

A safety tradeoff factor for all Army ground vehicles is whether bright (highway) headlights or blackout lights should be used in a combat zone. Table 2A-3 is an analysis of this problem.

2A-3.2 CONCLUSION

The disadvantage of using bright headlights in combat zones outweighs the safety advantages. The safety problems encountered when using blackout lights are known, but at this time there does not appear to be a reasonable alternative.

2A-4 UNDERCHASSIS CLEARANCE OF GROUND VEHICLES

2A-4.1 PROBLEM AND ANALYSIS

Another ground vehicle safety versus capability trade-off concerns the requirement for ground vehicles to have maximum off-road, rough terrain capability. A high underchassis clearance is necessary for rough terrain operation, but increasing the ground clearance raises the center of gravity of the vehicle and increases the risk of rollover. The advantages and disadvantages of increased clearance are given in Table 2A-4.

TABLE 2A-3. BRIGHT HEADLIGHTS VS BLACKOUT LIGHTS FOR ARMY GROUND VEHICLES

Advantages of Bright Headlights	Disadvantages of Bright Headlights
1. Personnel on foot on roadways can see approaching vehicles. 2. Drivers can better see the road and hazards. 3. Convoy discipline can be improved by maintaining greater intervals between vehicles.	1. The enemy can see bright lights and locate targets more easily. 2. Pedestrian traffic is partially "blinded" by bright headlights and loses some night vision until acclimated. 3. Because of better lighting, drivers tend to drive faster and become involved in more accidents.

TABLE 2A-4. ADVANTAGES VS DISADVANTAGES OF HIGH UNDERCHASSIS OF GROUND VEHICLES

Advantages of High Underchassis	Disadvantages of High Underchassis
1. Can negotiate rougher terrain. 2. Can ford deeper water than conventional vehicles.	1. Center of gravity raised; therefore, chance of rollover increased. 2. Stability in strong crosswind is reduced. 3. Design problems of the suspension system are increased.

2A-4.2 CONCLUSION

This problem does not have a simple decision of adopt or not adopt. The requirement is being met by increasing the underchassis clearance of combat vehicles. The question remains, "How much underchassis clearance is necessary?" As the clearance is increased, safety is traded for capability. Judgment—influenced by the statistics of accidents involving rollovers—must be brought to bear on this problem.

2A-5 EXAMPLES OF CONTINUING ARMY SAFETY VERSUS PERFORMANCE TRADEOFF STUDIES

2A-5.1 BATTLE SWITCHES

Battle switches are used in Army equipment to bypass or eliminate certain safety features. In this problem, the factors of safety provided by the design are balanced against gaining the capability of continued operation, even though under more hazardous conditions. A point of diminishing return is reached when bypassing a safety feature results in a more hazardous situation, even under battlefield conditions, than does simply failing to operate.

2A-5.2 LASER EQUIPMENT

Laser devices—designators or range finders—provide a valuable mission capability but endanger the eyes of friendly troops as well as those of the enemy. Although there are rules for the safe use of these devices and there are some safety features designed into the equipment, there does not appear to be any foolproof method to prevent inadvertent eye injury.

2A-5.3 CHANGES IN DESIGNS

Sometimes the design of an item will be changed to decrease its cost or to improve its producibility. Anytime a change is made in the design, the impact of the change on safety must be considered. It may be necessary to conduct a tradeoff study to determine whether the saving in cost or improved producibility is worth the decrease in safety caused by the change(s).

2A-5.4 UPGRADING EQUIPMENT

Sometimes instead of designing a new item of equipment to satisfy a mission need, the capability of an existing item of equipment will be improved by making changes to it. An example of this is placing a larger engine in a helicopter to increase its lifting capability. When making changes of this type to an item of equipment, the safety aspects of the introduction of the altered item must be closely examined to insure that additional safety problems are not introduced. In the example "Will the airframe accommodate the added weight and maneuverability?" must be considered.

2A-5.5 SYSTEMS BUILT FROM EXISTING SUBSYSTEMS

At times, to satisfy a mission need, several existing subsystems will be combined to form a new system. One such system was the SGT YORK. An existing radar, vehicle, and gun were combined to form this air defense system. When subsystems that have never been used together are combined, extreme care must be exercised to insure that one subsystem does not interact with another to cause safety problems and to insure that safety problems do not exist at interfaces of the subsystems.

PART TWO
SYSTEM SAFETY ANALYSES
CHAPTER 3
INTRODUCTION TO ANALYSIS

This chapter presents an introduction to system safety analyses. The need for analyses is presented, and the importance of conducting analyses early in the acquisition process is stressed. The methods and types of analyses are discussed. Uses of the results of system safety analyses are outlined.

3-1 NEED FOR ANALYSIS

Military Standard (MIL-STD) 882 (Ref. 1) defines a hazard as "a condition that is prerequisite to a mishap". It is important to think of a hazard not as an effect that will cause personal injury or equipment damage; instead, it is a condition. There are four main sources of hazards:

1. Hazardous characteristics of materials and equipment
2. Malfunctions of equipment
3. Adverse environments
4. Operator errors.

Hazards exist because at present there is no way to write specifications or other control documents that will result in completely safe systems. Designers can observe all of the stipulated safety requirements and still create unsafe designs. For this reason, there is a need to conduct safety analyses to locate the unsafe designs.

As equipment and systems became more complex, the need for formal safety analyses increased. The system safety engineering discipline evolved to satisfy this increased need for formal analyses and formal system safety programs. System safety engineers soon realized the importance of identifying and correcting hazards early in the life cycle of a system because it is expensive and ineffective to identify hazards only through investigations after accidents have occurred. Introducing design changes required to eliminate a hazard in a fielded system results in prolonged downtime and exorbitant cost. Consequently, safety analyses were developed to enable safety engineers to identify hazards while the system is still being designed, so that the design engineers could eliminate many of the hazards simply by changing their drawings before tooling has been ordered or hardware has been built. This approach is cost-effective.

Safety analyses are a systematic examination—started early in the acquisition process, often during the concept exploration phase—to examine the ways a system (or parts of it) will function in each operating mode, to identify potential hazards, to predict the potential of these hazards for injury to personnel or damage to equipment, and to determine ways to eliminate or reduce the hazard.

The objective is to eliminate or minimize the possibilities of accidents and their adverse effects before they can occur. Analysis is an effective and efficient evaluation technique that is supplanting the old "fly-fix-fly" method still used in some situations to determine the causes of accidents (Ref. 2).

The fundamental purpose of hazard analyses is to identify hazardous conditions so they can be eliminated or controlled during all life cycle phases. Hazard analyses reveal information about equipment designs and operation and maintenance procedures that cannot be obtained through any other reliable, practical means. The safety engineer uses the hazard analysis to determine how a system design is unsafe and how to correct this unsafe condition. If the hazard cannot be eliminated, the analysis may indicate the best measures for controlling it and for negating the adverse effects that not controlling the hazard can generate.

Analyses serve other, equally valuable purposes. They can establish either that a particular hazard does not exist or that the possibilities that accidents will result from the remaining hazards have been minimized or controlled to acceptable degrees. In addition, analyses can be used to verify that

1. The design complies with various requirements given in specifications, standards, codes, or other requirements documents.

2. Defective designs found in predecessor systems have not been repeated.

The advent of the system safety concept, and the resulting safety analysis, has generated sophisticated analysis techniques. For example, in the past weapon systems were developed without adequate consideration of user capabilities and limitations. Also developers failed to provide instructions that would enable users to cope adequately with accidents that might occur. To illustrate, safeguards may have been designed into the refueling of equipment or weapons with hazardous materials, but spills could still occur. Through the use of analyses, the remaining hazards can be further minimized. In the refueling example, analyses could identify—early in the

acquisition process—the requirement for accident-control instructions and for the provisioning of any additional safety equipment.

Safety analyses also serve to identify hazards associated with system interfaces. Many modern weapon systems are highly complex and, consequently, are developed by a combination of many different disciplines and organizations. When more than one design activity is involved, hazards not associated with any single subsystem may be present after the subsystems are combined. Even within the area of responsibility of one design activity, the same situation might exist between subsystems. Aside from identifying such potential hazards, analyses may serve as a basis for determining responsibilities of the various activities for bridging the safety interfaces, for development of safeguards, and in planning for safety tests to verify that interface problems have been resolved.

From the previous discussion it can be seen that the safety analysis is a basic tool of the system safety engineer. Specifically, he uses the data from the safety analysis in the following four principal ways:

1. To identify the hazards that do exist in a specific system and to eliminate from consideration all of the others that potentially could exist in all such systems

2. To determine the causes, effects, and interrelationships of existing hazards

3. To learn what elements of the system design will require preventive or corrective features and what those features might be

4. To identify any special tests that should be conducted with the prototype to verify safety features and to identify any additional system characteristics that could lead to accidents.

Because Army systems vary widely in technology and complexity, no one method of safety analysis is sufficient to evaluate whether every system or subsystem is safe. Furthermore, different types of analyses are needed during the various acquisition process phases. Therefore, several methods of safety analysis have been developed for specific purposes and for use at specific points in the acquisition of a system.

3-2 TIMING OF ANALYSES

The basic goal of safety analysis is to take preventive or corrective action before costly hardware changes are required. For this reason, analyses are most effective when begun early in the program. The changes to eliminate or control hazards can be incorporated with relative ease while the system design is still evolving. This is illustrated in Fig. 3-1. This figure shows that the total cost of correcting safety deficiencies increases rapidly during full-scale development and production and deployment and levels off to a constant, high figure during the operating and support phase, i.e., after all systems have been procured.

An old belief still subscribed to by some designers is that it is impossible to identify any of the safety problems in a new system until a prototype of that system has been built. This belief is erroneous for two reasons. First, current methods of safety analysis enable the safety engineer to recognize hazards while the system is being designed and developed. Second, although prototype testing is invaluable for some basic system safety activities, it is not ideal for hazard identification. Because of the controlled conditions and highly skilled personnel involved in prototype testing, accidents that would identify the hazards are not likely to occur. Therefore, there is no assurance that the hazards will be discovered. Defective designs are generally discovered through actual use only after large numbers of the system have been procured and placed in operation. By this time the cost of taking corrective action may be tremendous.

Safety analyses conducted prior to prototype testing may yield three major benefits:

1. If safety analyses are conducted early in the life cycle, hazards may be eliminated or controlled by changes made to the prototype design.

2. Analyses conducted just before prototype testing may identify potential hazards that still exist in the system and may suggest protective measures that should be taken during tests. An example is the discovery of excessive audio noise in a portable generator set; this discovery would result in the requirement that test personnel wear ear protection devices.

3. Analyses may identify the need for special prototype tests (a) to verify that the operational priority or sensitivity of a safety device is adequate for field conditions or (b) to identify the existence of unsafe system characteristics—such as equipment vibration—that could lead to accidents. An example of the former is the testing of an antitank recoilless weapon to verify the suitability of a safety interlock for preventing unintended firing during the loading operation.

3-3 METHODS AND TYPES OF HAZARD ANALYSES

Methods of safety analysis are the analytical techniques employed. Types of safety analysis are the categories of analysis prescribed by MIL-STD-882 and other sources. In some cases, any of several methods can be selected to perform a specific type of analysis.

Types of safety analyses and methods for conducting them were almost unknown until the US Armed Forces developed the system safety concepts and initiated system safety programs in the late 1950s. The types of analyses and methods for analysis were developed to satisfy requirements of system safety programs discussed in Ref. 2. Most of the methods and types were developed by Department of Defense (DoD) personnel or contractors to the DoD.
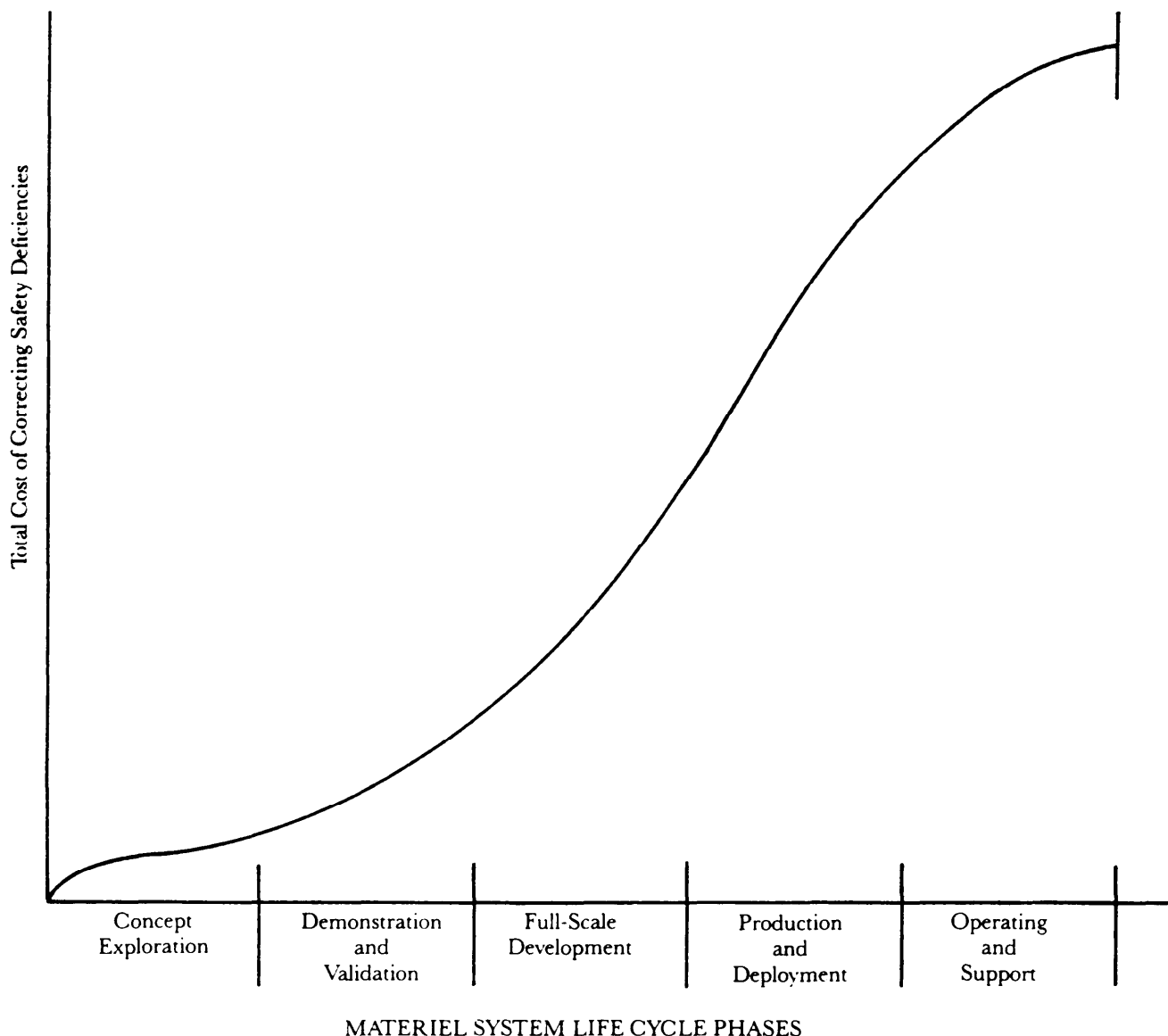
Figure 3-1. Relationship Between Total Cost of Correcting Safety Deficiencies and Life Cycle Phases

3-3.1 METHODS OF HAZARD ANALYSES

An analysis may be either qualitative or quantitative. A qualitative analysis examines events—the possible existence of hazards, the accidents that could result, possible effects, and safeguards. A quantitative analysis examines frequency or degree—the probability that particular hazardous events, accidents, and specific effects will occur. The quantitative analysis permits comparison of the changes in probabilities if safeguards or alternative designs are used in the system. A qualitative analysis must be conducted first to provide a point of departure for a quantitative analysis.

The applicability of quantitative methods is discussed here. Qualitative methods are described in par. 3-3.2, "Types of Hazard Analyses".

Results of quantitative analyses can be (1) *probabilistic*, using rate data, or expectancies, based on field experience or controlled laboratory testing, or (2) they can be *relativistic*, using comparison based on judgments.

Certain types of safety analyses lend themselves to quantification; others do not. When quantitative analysis is applicable, the relativistic method is most often used. Probabilistic methods are not yet widely used to predict the number of accidents that will occur, but they can be highly useful for comparison to indicate whether numerical safety design goals have been achieved and as a basis

for management decisions regarding proposed safety-related changes.

The limited use of quantitative methods to predict accident rates does not stem from any flaw in the methodology but instead from a shortage of valid input data. Probably the most accurate quantitative data available today are the failure rates of small electronic parts; those rates are often used in reliability analyses of entire assemblies or subsystems. However, those predictions are subject to error because failures in assemblies are caused less often by failures of the components themselves than by failures of the electrical connections joining them, which are due to environmental conditions, or by maintenance practices. Historical failure-rate data for large pieces of mechanical or electromechanical equipment are extremely rare. These data are necessary for accurate predictions of accident rates due to failures of similar equipment.

Although the data on failure rates of electrical and mechanical components and equipment are poor, quantitative values for other types of hazards—such as human error, environmental factors, and hazardous characteristics of equipment—are even less available or dependable. Laboratory tests have attempted to determine the probabilities that persons performing specific simple tasks will make errors, but the accuracy of the resulting data is questionable. In some cases the probability of the existence of a hazardous environmental factor might be roughly estimated. Also there appears to be no practical way to predict the probability that a piece of equipment will have hazardous mechanical characteristics, such as a sharp corner or edge, or pinch or squeeze points.

It has been found to be even more impractical to try to combine the probabilities of accidents from each of the contributing hazardous factors into a single, aggregate accident-rate value for the system. Only when comparable failure-rate data are available is the use of probabilities effective for comparing the accident rates of two systems of similar design.

Thus when the quantitative methods of safety analysis are examined in greater detail later in this handbook, it will be seen that the relativistic—or judgmental—forms are the ones most widely used at present. However, the Army is greatly interested in improving its safety-related system design goals. The Army also wants to develop more accurate risk assessment methods to provide its program managers with better information for making decisions about proposed design changes to reach those safety goals. Both of these objectives will require improved methods for predicting the probabilities of accidents. Accordingly, the probabilistic forms of the quantitative methods will gain importance as ways are found to improve the quantity and quality of the historical failure-rate data (both human and material) needed as inputs for computing accurate probabilities.

3-3.2 TYPES OF HAZARD ANALYSES

MIL-STD-882 (Ref. 1) identifies four types of hazard analyses: preliminary hazard analysis (PHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), and operating and support hazard analysis (O&SHA). Generally, each type is done at a different phase of the life cycle. In addition to these four types of analyses, the Army has introduced a fifth type—the software safety analysis.

Three techniques of analysis that may be used as part of an SSHA or SHA are identified in Ref. 1. They are fault hazard analysis (FHA), fault tree analysis (FTA), and sneak circuit analysis (SCA). Another analysis technique—not discussed in Ref. 1—for SSHA and SHA is the failure modes, effects, and criticality analysis (FMECA). The FMECA was developed for reliability analyses, but it also has value for safety analyses. Other techniques are identified in Table 3-1, categorized as to suitability for quantitative analysis. The techniques that are described in detail elsewhere in this handbook are marked with an asterisk. The critical incident technique is discussed in detail in Ref. 3. The Delphi Technique—a technique to obtain estimates—is discussed in Ref. 4.

A short discussion of the four types of hazard analyses identified in Ref. 1 is presented in the subparagraphs that follow.

3-3.2.1 Preliminary Hazard Analysis

The PHA should be initiated during the concept exploration phase of the life cycle. As the name implies, it is the first analysis of the system or system concepts. It is conducted to identify the hazards of the various system concepts being considered to satisfy a mission need. By using the best information available, the various system concepts are evaluated for hazard severity, hazard probability, and operation constraints. The results of the PHA are used in the evaluation of the various system concepts. Also the PHA establishes the framework for other hazard analyses. As the information concerning the system concept being considered to satisfy the mission need improves, the PHA should be updated. The PHA is discussed in greater detail in Chapter 4.

3-3.2.2 Subsystem Hazard Analysis

The SSHA is conducted to identify the hazards associated with the components of subsystems and the interfaces between components of subsystems. This analysis should identify all components whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The modes of failure of the components and the effects of component failures on safety should be identified during this analysis. Normally the SSHA should be conducted during the demonstration and validation phase; it should be initiated as

TABLE 3-1. ADDITIONAL (TO MIL-STD-882) SAFETY ANALYSIS TECHNIQUES

Analysis Technique	Quantitative	Remarks
1. Circuit Logic Analysis	Yes—When performed using Boolean logic	Mathematical techniques are similar to those for Fault Tree Analysis
2. Interface Analysis	Can have number relationships, but not a probability analysis	Physical, functional, or flow relationships support System Analysis
3. Mapping*	Can have number relationships, but not a probability analysis	Defines limits of hazardous areas, clearance dimensions, mutual interference problems, and machine-to-human interfaces
4. Monte Carlo Simulation	Yes—This is a mathematical technique primarily used for probability determination	Generally used to support some other analysis as a Fault Hazard Analysis or a Fault Tree Analysis
5. Contingency Analysis	Not generally, although specific situations can be quantified	Determines elements of reasonably foreseeable events other than normal situations
6. Environmental Factors Analysis	Can have number relationships, but not a probability analysis	Can be a separate analysis to be used to support any other safety analysis in which environment should be considered
7. Critical Incident Technique	No	Draws on past experience to support present safety analyses
8. Mock-Ups and Their Analysis*	No	Physical representation of design, which allows analysis by inspection and/or other means

*These techniques are described elsewhere in this handbook.

soon as detailed subsystem design information is available. The SSHA format should be selected carefully to simplify integrating the SSHA into the SHA. The SSHA is discussed in greater detail in Chapter 5.

3-3.2.3 System Hazard Analysis

The SHA is conducted to determine the hazards associated with subsystem interfaces. If possible, the same techniques used for the SSHA should be used for the SHA. Normally this analysis should be conducted during the full-scale development phase and starts as early in this phase as possible. Chapter 6 contains an expanded discussion of this analysis.

3-3.2.4 Operating and Support Hazard Analysis

The O&SHA is performed to identify the hazards associated with operating and supporting the system. This analysis is directly concerned with the safety consideration of the transportation, storage, maintenance, operation, and disposal of a system. The O&SHA should be started during the demonstration and validation phase and updated as the system progresses through the phases of the life cycle to disposal. It is especially important that any modifications or improvements made to a system

during the operating and support phase be analyzed to determine whether hazards have been introduced by these modifications or improvements. The O&SHA is discussed in greater detail in Chapter 8.

3-3.3 PROGRAMS OF ANALYSES

Methods and types of analyses have been addressed so far in this paragraph. Since the development of system safety, attempts have been made to find a single analysis that will satisfy all analysis requirements for all types of systems. Unfortunately, such an analysis has not been developed. A close examination of the information in subpar. 3-3.2 will reveal that the different types of analyses are designed to be initiated during the various phases of the life cycle and to satisfy the information needs during the various phases of the life cycle. There is, therefore, a need for a program of analyses. The AMC Supplement to Army Regulation (AR) 385-16 (Ref. 5) requires such a program.

Not all of the methods and types are applicable to all systems and during all phases of the life cycle. The selection of the method and type for a specific analysis becomes a matter of judgment for the analyst.

3-3.4 SELECTING VARIATIONS FOR SAFETY ANALYSES

Several types of safety analyses are described in general in this chapter and in detail in Chapters 4 through 8. Those analysis techniques that experience has shown are most beneficial and productive for system safety programs are included. Designers may use these analysis techniques to evaluate and to maximize the safety of systems being designed. Because system safety techniques are still under development, individual analysts should feel free to make variations and additions to the techniques to satisfy his or her particular purposes.

A general guide to developing variations is to examine the system concept or actual system to determine

1. The primary functional events that occur during normal mission operations
2. The forms of energy used
3. The way in which humans will become a part of the system
4. What unwanted events may occur.

Following this examination, select a technique or modify a technique as needed to satisfy the requirements of analysis. Functional hazard analysis, fault hazard analysis, procedures analysis, and human factors analysis are discussed in Ref. 6. Other techniques are addressed in Ref. 7.

3-4 ANALYSIS LOGIC

In selecting the best technique or techniques for use in a particular type of safety analysis, the safety engineer has certain criteria in mind. Two of these criteria are particularly important. First, he wants the analysis to be as comprehensive as possible, i.e., it should deal with as many of the hazards as can practicably be identified and evaluated. Second, he wants the analysis of each of the hazards to be as thorough and accurate as possible.

To satisfy these criteria, the safety engineer must select a technique of analysis that will enable him to use in the best way the system design detail available to him at the time. Accordingly, he must select the technique that uses the type of systematic approach that will enable him to use the available design detail. Systematic approaches will be discussed in greater detail following a discussion of the need for comprehensive safety analyses.

3-4.1 THE PRIMARY FUNCTION OF THE SAFETY ANALYSIS

The safety analysis usually provides several basic types of information:

1. Identification of hazards in the system
2. Identification of causes of the hazards
3. Prediction of the effects of the hazards
4. Recommendation of ways to eliminate or control the hazards.

The information provided by the safety analysis can be

of great value if the safety engineer

1. Selects the correct type of safety analysis so as to provide timely information
2. Selects the correct technique or techniques of analysis to provide the kinds of information that are needed
3. Selects the appropriate systematic approach to provide the needed amount of detail.

In system safety analysis, a systematic approach is one that will identify the maximum number of hazards in the system, identify their causes and predict their effects as accurately as possible, and recommend the most effective ways to eliminate or control the hazards. The need to use the correct systematic approach to a system safety analysis is the central theme of this discussion of analysis logic.

System safety analyses have many specific uses in the system safety program; some of them have been discussed previously, and others will be addressed in par. 3-5. Probably the most important use is that the analyses are the primary means by which the safety engineer informs the design engineers about the existence of safety problems in a system and recommends solutions to these problems. Because of the system safety analysis, the design engineers can get this information while they are still designing the system. Consequently, they can improve the safety of the system by changing the design before any hardware is fabricated. Such changes are relatively inexpensive.

There are two main reasons why design engineers need the information provided by the safety analysis. First, many design engineers are not experienced in identifying hidden hazards. Second, many design engineers are unaware that a definite set of priorities, or order of precedence, regarding the most satisfactory ways to resolve hazards (discussed in greater detail in par. 3-4.3) have been established. Well-executed safety analyses will provide precisely the guidance that is needed by the design engineers.

3-4.2 THE NEED FOR SYSTEMATIC IDENTIFICATION OF HAZARDS

No system can be made perfectly safe. There are too many variables; therefore, it is impossible to eliminate every possible hazard. However, it is very important to eliminate or control as many hazards as is practicable. But before any hazard can be resolved, it must first be identified, and its cause(s) and effect(s) analyzed.

Sometimes accidents happen because design engineers fail to identify and eliminate or control a serious hazard. This occurs because designers have little or no education and experience in system safety principles and methods and, therefore, can only recognize those hazards that are immediately apparent. They fail to recognize the hidden hazards.

The design engineer may identify a hazard involving a single point failure—a single condition, such as a material

failure or an operator error, that can directly cause an accident. However, he may overlook a "common cause condition" that can have multiple effects that lead to an accident. An example is susceptibility to wire bundle damage where multiple shorts in the wires can do damage. Similarly, the design engineer might overlook two or more seemingly unrelated conditions that can interact to cause an accident.

Sometimes the effects of hazards can be difficult to identify. For example, when asked what hazards exist in homes because of electrical power, numerous engineers mention the possibilities of shock and fire. They generally · fail to think of other accidents that can result, such as,

1. The effects of damage caused by power failure

2. Damage and burns caused by overheating

3. Injury or damage from inadvertent activations or electrical explosions, e.g., violent disruptions of an electrical conductor because of a high-current short of a small diameter wire.

Because of problems of identifying hazards and of finding hidden hazards, most design engineers can benefit greatly from a timely safety analysis that identifies all identifiable hazards, their causes, and their effects. If the system safety engineer is to provide a quality analysis, he must use the correct systematic approach and have a good working knowledge of the precedence in selecting ways to eliminate or control hazards.

3-4.3 SAFETY ACTION PRECEDENCE

MIL-STD-882 (Ref. 1) gives the order of precedence for satisfying system safety requirements and resolving identified hazards as follows:

1. "Design for Minimum Risk. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA [managing activity], through design selection."

2. "Incorporate Safety Devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable."

3. "Provide Warning Devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems."

4. "Develop Procedures and Training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver, no warning, caution, or other form of written advisory shall be used as the *only* risk reduction method for Category I or II hazards.... Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the MA. Tasks and activities judged critical by the MA may require certification of personnel proficiency.".

In the past designers often used the easy solution of specifying an operating or maintenance procedure to control a hazard rather than using good design to eliminate it. For example, if Operation A must be performed before Operation B to prevent a hazardous situation, but the design of the system allows either operation to be performed first, the design is unsafe. In this situation the design engineering is relying on correct procedures to insure safe operation; this should be corrected.

In each case the safety engineer should determine whether the designer has done as much as possible to eliminate or control any hazard that might cause unsafe operation or whether he has simply chosen an easy solution by specifying a procedure.

3-4.4 ANALYSIS APPROACHES

To provide maximum system safety, the system safety engineer must provide the design engineer with all possible information about the hazards of the system. To do this, the safety engineer must use a systematic approach or approaches when making the analyses.

When performing safety analyses, safety engineers use one or more of the systematic approaches that follow:

1. *End Effect*. A possible undesirable end effect is selected. This is usually a specific accident. All of the factors that could cause the accident or contribute to the cause of the accident are identified. Next, the possible causes of those factors are identified. The best known and most frequently used form of analysis of this type is the fault tree analysis.

2. *Hazard Evaluation*. The hazards that might be present in a system are identified by review of the characteristics of the system, e.g., a system that uses electrical power may be expected to have certain electrical hazards, which can be identified using information such as that provided in Chapter 10. Each hazard is evaluated for

a. The probability that the hazardous event will occur

b. The effect that the hazardous event would have on personnel

c. Possible safeguards to prevent the occurrence of the undesirable event.

3. *Bottom Up Sequence*. A system is broken in subsystems, assemblies, and components. By beginning at the lowest level, each is analyzed until all components,

assemblies, subsystems, and the system have been studied. The FMECA is an example of an analysis technique that employs a bottom-to-top-type systematic approach.

4. *Top-Down Sequence*. The system is analyzed first, then the subsystems, assemblies, and eventually, the components of the system are subjected to a system safety analysis. Generally, the preliminary hazard analysis can be done only from the top to the bottom since little detail is available below the system or subsystem level in the early part of the acquisition process.

5. *Magnitudes of Energy*. The amount of damage and number of injuries that can result from an accident are often in proportion to the uncontrolled energy released in the system. To use this approach, the sources of energy are analyzed in descending order; the system safety engineer first evaluates the most powerful source of energy in the system that can cause or contribute to an accident. Next the second most powerful source is evaluated, etc. Some system safety engineers believe that all potential hazards in a design can be analyzed through energy analysis. This approach, however, depends upon defining every potentially hazardous event in some manner related to energy, e.g., for a finger cut on a sharp edge, the muscle moving the finger is the form of energy. A toxic substance acting on a body should be defined as a form of chemical energy. This approach does not lend itself readily to comprehensive analysis.

6. *Checklists*. To insure that the safety requirements from specifications, standards, and other documents are satisfied, checklists of these requirements are used by designers and system safety engineers. The system safety checklists cover only those parts of the specifications, standards, and other documents that have system safety connotations. The specifications and standards are often based upon common experiences with accident-prone systems and were written in an attempt to eliminate the hazardous characteristics from new systems. The checklists are another form of hazard identification and evaluation. Although they are not specific examples of systematic approaches for system safety analyses, they do supplement such approaches and should be used whenever they can be developed from applicable information.

3-5 USES OF ANALYSIS RESULTS

Specifically, the results of safety analyses can satisfy the reporting requirements of Data Item Description (DID) No. DI-H-7048 (Ref. 8). This document contains specific guidance concerning the information that must be reported for each type of system safety analysis.

On a broader basis, the results of the system safety analyses can be used to continue the safety process that will lead eventually to an acceptably safe design. Whether the analyses indicate that the initial design is safe or hazardous, the results are significant. However, analyses identifying hazards are useful only to the extent that

action is taken to eliminate or control those hazards. Thus it is incumbent on the safety group to follow up the analyses. Failure to do so would result not only in a complete waste of the system safety analyses but also in a system design that is unsafe.

3-5.1 ANALYZE FOR SAFETY

Safety analyses done early, especially those accomplished before the system design has progressed much beyond the concept exploration phase, can provide useful guidance for implementing safety features, eliminating or controlling hazards, and developing safety criteria. The safety deficiencies revealed by these early analyses generally can be corrected at a much lower cost than would be the case later in the program. However, analyses conducted later, i.e., during and after the design stage, can also provide benefits. These benefits are discussed in the paragraphs that follow.

3-5.2 INDICATION OF SAFE DESIGN

When an analysis indicates that a system is acceptably safe and requires no corrective actions, a salutory result has been achieved. Determining that a specific hazard does not exist within a piece of equipment or an operation, or that a hazard does exist but has been suitably controlled, is as positive a result of a safety analysis as is determining that a defect or lack of control exists. The process of performing a systematic safety evaluation of a system for a safety analysis provides the safety engineer with much useful information because in essence he is asking a large number of structured "What if?" questions.

An analysis that indicates an acceptably safe design often can be put to further uses. In many instances the original analysis may show that although the design of the system is safe, care must be taken during production to prevent degradation of the safety designed into the system. This is especially important when the analyses indicate that a material substitution or other change could cause a failure that could result in an accident. In such cases the safety engineer must transmit the results of the analyses to the production and quality control personnel to guide them in taking suitable actions to prevent safety degradation.

The results of analyses that indicate no apparent safety problems can be helpful to personnel other than those in production and quality control. Some examples are

1. Personnel involved in the planning and/or conducting of system or subsystem tests can be informed of actions to be avoided, safeguards to be observed, and system safety features designed to prevent accidents during testing.

2. Writers of technical manuals for system operation and maintenance can be informed of special procedures, cautions, and warnings required for safe operation of the system that must be included in the technical manuals.

Guidance concerning the inclusion of safety information in technical manuals is given in Refs. 9 and 10.

3-5.3 INDICATION OF DESIGN DEFECT

As important as analysis results can be when no design defect is found, the results are equally important if they indicate that a hazard exists that has not been controlled adequately. When a hazard is found, the design group must respond with corrective action, which must include, if necessary, tradeoff studies of safety versus other considerations, or the entire safety analysis will have been wasted.

The vehicle by which the safety engineer insures the proper response to his analysis and recommendation is the hazard report. A recommended form for reporting hazards is shown in Fig. 3-2.

The hazard report is a formal, written statement of a hazard that can be sent not only to the responsible design group but also to other groups that may have an interest in the hazard. The form shown in Fig. 3-2 provides a means of not only documenting the hazard but also of recording the action taken to eliminate or control the hazard. The safety group should follow closely each report until a date has been entered in Block 10 indicating that the hazard has been eliminated or controlled. If used properly, the form will have the entire history of a hazard in one report. The file of completed reports provides a valuable source of "lessons learned".

3-6 SUMMARY

It is easy to see why the safety analysis is the most important tool available to the safety engineer. He uses the initial analysis to evaluate systematically the safety of the initial system design. He uses the data from the early analyses to recommend specific changes to improve the safety of the system when the changes can be incorporated economically into the emerging design. He uses later analyses to verify that the safety has been improved through those changes and to recommend additional changes to minimize or control those hazards that could not be eliminated.

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirement*, 30 March 1984.

2. SAMSO-STD-68-8B, *Methodology for System Safety Analysis*, Space and Missile Systems Organization, Los Angeles, CA, 11 August 1977.

3. William E. Tarrants, *The Measurement of Safety Performance*, Garland STPM Press, New York, NY, 1980, pp. 301-78.

4. D. Frend and J. T. Hawkins, *The Delphi Technique, Weapon Systems Safety Supervision*, Naval Weapons Laboratory, Dahlgren, VA, May 1982.

5. AMC Supplement 1, *System Safety Engineering and Management*, to AR 385-16, 3 March 1987.

6. J. M. Brush, R. W. Douglass III, F. R. Williamson, *A Guide for Performing System Safety Analysis*, NASA-TM-X-64799, George C. Marshall Space Flight Center, Marshall Space Flight Center, AL, 18 January 1974.

7. W. Hammer, *Product Safety Management and Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

8. Data Item Description, DI-H-7048, *System Safety Hazard Analysis Report*, 1 May 1984.

9. MIL-M-38784B, *Manuals, Technical: General Style and Format Requirements*, 16 April 1983.

10. MIL-HDBK-63038-1A (TM), *Technical Manual Writing Handbook*, 15 May 1984.

BIBLIOGRAPHY

D. E. Allmand, *et al., Relative Accident Probability Analysis*, NAVORD Report 4135, Naval Ordnance Laboratory, White Oak, MD, November 1955.

J. L. Clark, *The Management Oversight and Risk Tree (MORT)—A New System Safety Program*, US Atomic Energy Commission, Washington, DC, February 1973.

R. A. Duregger, E. Leon, and J. R. Sample, "System Safety Analysis Techniques as Applied to Shipboard Systems", *Proceedings of Society of Naval Architects and Marine Engineers Spring 1972 Meeting*, New York, NY, May 1972.

W. Hammer, *Numerical Evaluation of Accident Potentials*, Institute of Aeronautics and Astronautics Symposium on Reliability and Maintainability, New York, NY, July 1966.

1. Hazard Report No.	5. Submitted By	8. TO: Action:	9. Source:

Design Review ☐

Analysis ☐

Inspection ☐

Field Report ☐

Test ☐

Other (specify) ☐

2. Date Report Initiated

6. Address

3. System

Information:

7. Telephone No.

4. Subsystem

10. Date Hazard Eliminated or Controlled

11. Subject

12. Description of Problem (Include cause and effects)

(continue on reverse side if necessary)

13. Requirements (Include paragraph number of specification, standard, etc.)

(continue on reverse side if necessary)

14. Current Probability of Accident

(continue on reverse side if necessary)

15. Recommended Solution

(continue on reverse side if necessary)

16. Summary of Actions to Eliminate or Control Hazard

(continue on reverse side if necessary)

Figure 3-2.   Hazard Report Form

CHAPTER 4
PRELIMINARY HAZARD ANALYSIS

This chapter contains detailed information on the preliminary hazard analysis (PHA). It describes the formats for presenting PHA information. The techniques for determining hazards, which include potential generic hazard analysis, mission analysis, hazard plotting, and mock-ups, are discussed. Sources of data are indicated, and limitations of the PHA are discussed.

4-1 PURPOSE AND DESCRIPTION

The preliminary hazard analysis (PHA) is the first of a series of safety analyses conducted during the life cycle of a system or item of equipment. It should be conducted as early as possible in the life cycle. If possible, it should be initiated during the concept exploration phase. The PHA should examine the safety of each alternative that is being considered to satisfy the military need. The purpose of the PHA is to provide early guidance to designers, managers, safety engineers, and other interested personnel on the potential hazards of each of the alternatives.

During the concept exploration phase, the PHA can provide information valuable in conducting tradeoffs among the various alternatives. The next use for the PHA is during the demonstration and validation phase. Normally just prior to the start of this phase one of the alternatives being considered is selected, and the design of the system or item of equipment is started. However, before the design is actually started, the designers should study the PHA to learn what the potential hazards are and how, through design, these hazards can be eliminated or minimized.

Military Standard (MIL-STD) 882 (Ref. 1) states that as a minimum the items that follow shall be considered for the identification and evaluation of hazards:

"a. Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).

"b. Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls).

"c. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and nonionizing radiation including laser radiation).

"d. Operating, test, maintenance and emergency procedures (e.g., human factors engineering, human error

analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage).

"e. Facilities, support equipment (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; radiation or noise emitters; electrical power sources) and training (e.g., training and certification pertaining to safety operations and maintenance).

"f. Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, hardware or software fail-safe design considerations, subsystem protection, fire suppression systems, personal protective equipment, industrial ventilation, and noise or radiation carriers)."

A carefully executed PHA should provide the information that follows:

1. Specific potential hazards in a proposed system

2. The probable magnitude and frequency of each adverse effect to a proposed system with and without the recommended safeguards. This information can be used in tradeoff studies of alternatives.

3. Proposed measures to eliminate or control the potential hazards

4. The safety-critical equipment and situations upon which the designers must focus their hazard elimination or control efforts

5. Potential events (accidents) that should be subjected to detailed analysis when additional information becomes available

6. Potential personnel errors that can lead to accidents avoidable by design features such as interlocks, warnings, and procedural instructions

7. Identification of specific safety essentials that satisfy requirements in standards, specifications, or similar documents

8. Notes on accidents, near-misses, and other poten-

tial safety problems uncovered during experience with predecessor systems

9. Potential hazards whose control should be verified through specific safety testing.

Item No. 5 in the previous paragraph can be a very important result of a PHA. If the parts or operations of a system that may be hazardous are identified through the PHA, detailed analyses can then focus on these parts or operations. However, if the parts or operations of a system that may be hazardous are not identified through the PHA, it will be necessary to conduct detailed analyses of the entire system—a costly undertaking.

The PHA is also used in preparation of the Preliminary Hazard Analysis Report, which is described in Data Item Description (DID) DI-H-7048 (Ref. 2). This DID identifies the information that the report must include to document the analysis of the system under consideration. The report should become the written record of the PHA and any pertinent, related information.

Each hazard identified in the PHA should be documented in a hazard report. This report, including a suggested form, is discussed in par. 3-5.3. The hazard report provides a vehicle for following a hazard until it is eliminated or controlled.

4-2 ANALYSIS CONTENT

The PHA should be as useful as possible in identifying potential hazards and in indicating means of corrective action. Therefore, the previously stated items from MIL-STD 882 (Ref. 1) must be considered even though not all of the items will relate to every system being analyzed, but each must be considered to insure that none is inadvertently omitted.

Since the initial PHA is started early in the system life cycle, the information in the analysis usually will be rather general and will provide little detail. Nevertheless, this preliminary information can contain enough indication of the potential hazards and resulting effects to alert designers to the need for corrective action through design. For example, it is known that wherever electricity is used certain electrical hazards are possible. Thus knowledge that a system or subsystem will be electrically powered enables the safety engineer to make an early evaluation of potential adverse effects so that measures to prevent or minimize accidents can be incorporated into the system design.

The amount of information available for a PHA will depend in part on whether the system to be analyzed is entirely new in concept or whether experience data can be derived from predecessor systems. In some cases, new systems use subsystems, components, or materials from, or similar to those from, previous systems, and information about these subsystems, components, or materials will be useful in the PHA.

The exact content of the PHA is not specified. The list

of specific information given in par. 4-1 furnishes some guidance concerning content, and DID DI-H-7048 (Ref. 2) provides additional guidance by stating what the PHA report must contain. The required elements of the PHA report will be discussed in detail in par. 4-3.1.1.

4-3 ANALYSIS FORMATS AND TECHNIQUES

The format and techniques that the analyst selects in making a PHA will depend to a great extent on the complexity of the system, the analyst's personal preferences, the types of information to be presented, and the depth to which the analysis will delve. Also the PHA must be integrated into and be compatible with the efforts of the other disciplines and activities involved in the program.

4-3.1 ANALYSIS FORMATS

The two types of PHA in common use are tabular and narrative. The analyst may use either or both of these formats.

4-3.1.1 Tabular Format

The tabular format is most commonly used for the PHA. The exact composition of the tables may vary with the personal preferences of analysts and with the types of information to be presented. As previously stated, when a PHA report is to be prepared in accordance with DID DI-H-7048 (Ref. 2), specific categories of information must be provided. Except for the required summary of results, all the reporting requirements in DID DI-H-7048 can be satisfied by the tabular format. A list of requirements from DID DI-H-7048, which become the column headings, and a brief description of each requirement follow:

1. *System/Subsystem/Unit*. This information will describe the particular part of the system with which this element of the analysis is to be concerned. Every analysis report sheet must identify the part of the system being considered, but the presentation may vary. Some analysts list the system description at the top of the sheet and provide a column that tells which subsystem contains the hazard. Other analysts prepare separate sheets for each subsystem and list the subsystem identification at the top of the sheet. Subsystems or lower divisions of the system must all be given positive identification, e.g., power supply number 1 or fuel subsystem.

2. *System Event(s) Phase*. In this column the state of the system is identified. Examples of system states are mission performance, maintenance, repair, transportation, or storage. Some states may have substates. Mission performance of an aircraft might be divided into taxiing, takeoff, flight, and landing.

3. *Hazard Description*. A brief description of the

hazard should be given and should include the various ways in which the hazard could become apparent. Also this column should contain information on whether the hazard is caused by normal operating conditions or by a failure or other abnormal condition.

4. *Effect on System.* In this column are listed the adverse effects that could result from the hazard. The information should identify clearly the probable injuries to specific groups of people, e.g., maintenance personnel or bystanders, and probable damage to equipment and/ or property that could result if no safeguard is included.

5. *Risk Assessment:*

Complete risk assessment requires determining the severity of a hazard and the probability that the hazard will occur. When the PHA is done before system design, normally only the severity of the hazard is needed because if at all possible, the hazard will be eliminated through design. If the design does not eliminate the hazard, information concerning severity and probability is needed to establish priorities for actions to control or minimize the hazard.

Hazard severity categories have been established to give a qualitative measure of the worst credible mishap that could result from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. The hazard categories are given in Table 4-1; they offer general guidance for a wide variety of programs. However, it may be necessary for a specific program to define a mishap in more detail. As examples, it may be necessary to define what constitutes system failure, major system damage, minor system damage, or occupational illness.

A quantitative hazard probability cannot be determined until a system is manufactured and used for

some time. Quantitative probabilities may be of value for considering the hazards of future systems that are similar to the system being considered or being designed, but they are of no value to the present system. Through experienced engineering judgment and/or evaluation of historical safety data from similar systems, qualitative hazard probabilities may be established. Table 4-2 is a listing of qualitative probability rankings. Since qualitative rankings are subject to individual interpretation, it is very important that the rationale for all qualitative hazard probabilities be adequately documented in the report.

6. *Recommended Action.* Means should be recommended to eliminate or control the hazard. Since the PHA is started early in the acquisition process, all possible means to eliminate or reduce a hazard should be given. The safeguards used in previous systems should be addressed, and safeguards recommended or required by

TABLE 4-1
HAZARD SEVERITY CATEGORIES (Ref. 1)

Description	Category	Mishap Definition
Catastrophic	I	Death or system loss
Critical	II	Severe injury, severe occupational illness, or major system damage
Marginal	III	Minor injury, minor occupational illness, or minor system damage
Negligible	IV	Less than minor injury, occupational illness, or system damage

TABLE 4-2
HAZARD PROBABILITY RANKINGS (Ref. 1)

Description*	Level	Occurrence Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in the life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely it can be assumed occurrence may not be experienced	Unlikely to occur but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

military documents (Army regulations, military standards, etc.) should be included where appropriate. When possible, the cost impact of the various safeguards should also be given.

7. *Effect of Recommended Action*. This column is used to document the improvement in the risk assessment if the action recommended in the previous item is taken.

8. *Remarks*. Any information the analyst believes pertinent and is not covered in other columns may be added here. The information in this column may include applicable documents, previous failure data on similar systems, and administrative directions.

9. *Status*. The status of implementing the recommended hazard controls will be listed in this column.

Useful information not required by DID DI-H-7048 can be inserted in additional columns as desired by the analyst. Some of the column headings that could be used follow:

1. *Numerical Indicator*. Usually the first column in the table lists item numbers, and often subitem identifications are also listed. The item numbers provide an effective reference system for the entries in the table.

2. *Reference Material*. This column may be added to list appropriate reference material, which may include information from other analyses, test reports, specifications, standards, and codes.

3. *Lessons Learned*. Safety-related information obtained from previous systems that can be associated with a specific hazard in the system under consideration or development should be entered in this column. This includes information on accidents, near-misses, failures, and related experience.

4. *Future Analysis Indicators*. This column should contain recommendations for future analysis of a specific hazard. As an example, if the PHA reveals that a component or subsystem could cause an accident, a recommendation is entered in this column for a failure modes and effects analysis.

5. *Responsibility*. This column can be used to identify specific persons or organizations responsible for taking action to eliminate or reduce a given hazard.

Fig. 4-1 is an example of the tabular layout using the previously described headings. The column headings for a simpler PHA are shown in Fig. 4-2. The format of Fig. 4-1 is probably most useful for large, complex systems, such as tanks, radar control gun systems, and large radar systems, whereas the format illustrated in Fig. 4-2 is probably most useful for relatively simple systems, such as pistols, rifles, mortars, or towed artillery.

4-3.1.2 Narrative Format

Sometimes the tabular format may be undesirable or inadequate for the type of material to be analyzed. Tables can present considerable information in condensed form, but in some cases, a narrative format will be more effective.

Usually the narrative format is laid out so that each part of the analysis addresses a major safety subject, and the paragraphs and subparagraphs address the subcategories of that subject. For example, the possible occurrence of a fire can be evaluated in detail by using the narrative format of the PHA. The first part of the PHA may discuss the fire itself. A fire requires three things—namely, fuel, oxidizer, and heat. Each of these may be discussed in a separate paragraph. Within the paragraph on fuel, all of the fuels that could be present, the characteristics of these various fuels, the amount of energy required by each fuel for ignition, and the fuels considered most hazardous may be discussed. Other parts can address methods of fire prevention, fire detection devices, firefighting equipment, and other relevant information.

Some reasons for selecting a narrative format follow:

1. To insure that the items that should be considered for the hazards listed in par. 4-1 are completely discussed. Each of the items should be evaluated for hazards, and if no hazards exist, this fact should be stated.

2. To provide a detailed discussion to satisfy the requirements of DID DI-H-7048 (Ref. 2). Such a discussion might explain the need for acceptance of certain hazards because of mission or other requirements. Also text may explain how a proposed concept can avoid safety problems that existed with similar predecessor systems.

3. To present detailed data and facts that will not fit in a tabular format. For example, a tabular presentation may indicate fire is a possible hazard in a proposed system. However, tabular format would not provide for all the details that can be presented in narrative form.

4. To discuss the relative safety of the system, subsystem, or component being analyzed. The narrative format may be more suitable than the tabular one for discussing a tradeoff between designs—with and without safeguards—that could be selected.

5. To describe the system, subsystem, or component being analyzed so the reader can understand more readily the circumstances under which the hazard can exist, the factors that can cause the hazard, and the adverse effects that can result.

4-3.1.3 Combined Formats

In some cases it may be desirable for a PHA to use a combination of the tabular and narrative formats. The tabular format can be used to present summarized information, and the narrative format can be used to present an expanded discussion of the summarized information. Each narrative element should include the corresponding numerical indicator from Column 1 of the tabular portion to coordinate the two formats.

Item No.	Subsystem or Unit	System Event(s) Phase	Hazard* Description	Effect* on System	Lessons Learned	Risk* Assessment	Recommended* Action	Effect of* Recommended Action	Reference Material	Remarks*	Future Analysis Indicators	Responsibility	Status*

Required by DID DI-H-7048

Figure 4-1. Example of PHA Tabular Form That Satisfies Requirements of DID DI-H-7048

PRELIMINARY HAZARD ANALYSIS

SYSTEM:

Item No.	Hazardous Condition or Event	Hazard Severity Category	Cause	Effect	Safeguard	Probability of Occurrence if Safeguard Is Implemented	Remarks

Figure 4-2. Example of a Simpler PHA Format

4-5

4-3.2 ANALYSIS TECHNIQUES

Par. 3-4.4 presents several systematic approaches for use in performing safety analyses. These approaches were developed to avoid omission of any hazards, equipment, conditions, or events that should be considered in the safety analysis. The approaches that apply to the PHA are discussed in the paragraphs that follow.

4-3.2.1 Top-Down Sequence

In this approach the analysis is started at the system level, progresses to the subsystem level, and then to the unit level. The unit being analyzed is studied to identify all the hazards it can generate or to which it might be subjected. The lowest level at which this approach can be used depends on the level of information available to the analyst at the time the PHA is conducted. When the design is complete or near completion, the analysis can be extended to the lowest level and developed into what will become a fault hazard analysis (FHA).

4-3.2.2 Generic Hazards

In this approach the analyst considers generic hazards—those hazards that might be expected to be in the equipment because of the technical nature of it—to determine whether they exist in the specific system, subsystem, or component being analyzed.

Each system will have certain hazards that are inherent in the design or in the sources or uses of energy. The types of generic hazards that should be used in determining the potential hazards for a PHA are discussed in Chapter 10.

Depending on the current and voltage involved, a system using electricity may or may not have the types of hazards generally associated with electricity. When fluid pressure is used, other potential hazards may exist. These hazards depend on whether the fluid is a gas or liquid, the type of gas or liquid, and the pressures involved.

The stated requirements for safeguards against potential generic hazards provide clues as to what hazards to expect in a particular system. These requirements are often contained in standards or system specifications. Many of these safety provisions were incorporated into the various documents because either a preliminary analysis indicated accidents could occur or accidents did occur when using the system. Thus a requirement for a guard over the moving parts of a piece of equipment indicates that the moving parts are considered hazardous, and this gives an indication of where to look for similar hazards in new designs.

For a system or subsystem with numerous potential hazards, the question arises as to which hazards should be investigated first. As long as all hazards are addressed, the end result will be the same. Nevertheless, it is best to start with the most significant hazard, i.e., the one that can cause the greatest number of injuries or greatest amount of damage. Generally, the most significant hazard will occur from an uncontrolled release of the largest amount of energy in the system.

Usually, the release of energy from explosives will be the most potentially destructive. Therefore, if an analysis is conducted on a system or subsystem that contains an explosive, the hazards due to the explosive should be examined first. The second hazard to be considered should be the possible explosions that could result from substances usually not regarded as explosive—such as highly reactive materials—and that release energy in great quantities very quickly. Analysis of potential fire sources may follow next. This precedence of hazards would continue to hazards, such as toxic materials, that could cause injury or damage but are less energetic.

Problems with predecessor systems can provide insights into potential hazards that should be included in a PHA. Operators and maintenance personnel of predecessor systems can provide their experiences with the systems and their knowledge of the experiences of others. Accident records of predecessor systems may indicate the types of hazards that may exist in the system under investigation. For information about the sources of these records, see par. 4-4.

4-3.2.3 Subordinate Analysis Routines

Inputs to the PHA can be generated by subordinate analyses, such as mission analysis, plotting of hazards, and mock-ups. Early use of these subordinate analyses permits evaluation of situations that could be hazardous and of the safety measures that could be incorporated into the system. Subordinate analysis routines will be required when the design data alone are insufficient to enable the safety engineer to evaluate suspect hazards adequately. Some of these routines are discussed in the paragraphs that follow.

4-3.2.3.1 Mission Analysis

Mission analysis is a study of the tasks a system must perform, the ways the system must operate, and the environment in which the tasks must be performed. A part of the requirements documents for a new system is a statement of the mission of the system and an operational concept of the system. Included in the operational concept will be a discussion of the environments in which the system must operate.

The mission statement and operational concept must be studied to determine the tasks that must be performed to accomplish the mission of the system. Each task must be studied to determine the hazards associated with it and ways of eliminating or reducing the hazards. The environments in which the system must operate must be considered because the hazards may change with environment.

4-3.2.3.2 Plotting of Hazards

Another technique to determine hazardous conditions for a PHA is the plotting of the location of hazardous parts or parts containing hazardous materials. After the locations are plotted, they are analyzed to determine the hazards present and ways to eliminate or reduce the hazards.

An example of the value of plotting follows. The gasoline tank for the motor of an electrical motor-generator set was placed above the motor. It was often necessary to fill the tank while the motor was running since the motor cannot be stopped. During the fueling operation, gasoline spilled on the exhaust manifold and ignited. Had the location of the gasoline tank and exhaust manifold been plotted during the PHA, the hazardous condition would have become obvious to the safety engineer.

Plotting the locations of system parts is not the only type of plotting of value during a PHA. Other types of plots valuable during the PHA include

1. Radiation from radars, lasers, and similar microwave equipment, which indicates the limits of hazardous radiation

2. Noise-level contours to determine whether specific pieces of equipment require noise insulation

3. Exhaust pattern from rocket motors

4. Limits of movement of mechanical parts in relation to other parts or personnel.

4-3.2.3.3 Mock-Ups

Mock-ups are three-dimensional simulators built to show the space that persons and equipment will occupy and the relationship between the two. Generally, they are made of inexpensive materials, such as cardboard or wood.

At first glance, mock-ups—like plotting—may seem inappropriate for a PHA; however, in fact, they allow the safety engineer to identify certain space- and location-related hazards very early in the system acquisition process when changes can be made easily and at low cost. Mock-ups may be used effectively to determine

1. Whether a driver has adequate room to operate a vehicle without hitting his head on a hard surface or, wearing protective clothing, he has adequate room to operate brake and clutch pedals

2. Whether an individual can reach and operate an emergency switch from his location

3. Whether a vehicle opening is adequate for persons wearing protective clothing and equipment

4. Whether a vehicle opening is adequate for people to escape through in an emergency

5. Whether maintenance personnel can see and reach a part that may require repair or replacement.

Mock-ups—like some other techniques used by the safety engineer—are of value to other engineering disciplines. The examples previously given in this paragraph could serve the needs of the human factors engineer and the maintainability engineer.

4-4 SOURCES OF DATA

There are two basic types of data needed to conduct a PHA. The first type is the requirements data, such as the maximum level of noise to which a human may be exposed, the maximum exposure of humans of x-radiation, and the maximum surface temperature of exposed metal in the vicinity of humans. These requirements data are set down in Government publications such as military standards (MIL-STD), technical bulletins (TB), and Occupational Health and Safety Administration (OSHA) standards.

The second type of data has to do with the identification of a hazard and the probability it will occur. Historical information about predecessor systems is a major source of such data. A list of DoD sources of historical-type data is contained in par. 2-3; and a list of both source and the type of data available from organizations is presented in Appendix 4A. The sources in Appendix 4A are grouped by safety data and reliability data; both are given since there can be a strong correlation between reliability and safety. Another source of historical data is the manufacturer of the system or the contractor performing a study of a new system. Data from manufacturers or contractors should be carefully analyzed because it is only natural that a contractor or manufacturer will tend to stress the positive features of his product and minimize the negative ones.

4-5 EXAMPLE

An example, from Ref. 3, of a PHA, using the tabular format of Fig. 4-2 (that of Fig. 4-1 could also be used), is shown in Fig. 4-3. The PHA was performed for two principal reasons: (1) to determine whether the weapon being tested for acquisition purposes has undesirable characteristics that may injure personnel and (2) to indicate the precautionary measures to be taken by test and evaluation personnel to avoid injury during testing.

4-6 GETTING AROUND LIMITATIONS

The preliminary hazard analysis is accomplished early in the program when detailed information is not available. As the design progresses, many changes are made, and some of those changes may introduce hazards not envisioned in the early PHA. In addition, changes in mission and/or more accurate later data concerning mission will also affect the results of the original PHA. Therefore, the PHA generally will be inadequate to identify all the potential failures or errors that can initiate sequences of events that could lead to an accident. For such purposes, detailed analyses—such as the fault tree analysis (FTA) and the failure modes, effects, and criticality anal-

PRELIMINARY HAZARD ANALYSIS

SYSTEM: M-102 RIFLE

Item No.	Hazardous Condition or Event	Hazard Severity Category	Cause	Effect	Safeguard	Probability of Occurrence if Safeguard Is Implemented	Remarks
1A	Projectile impacts in occupied area.	Catastrophic	Weapon is intentionally fired unknowingly into an occupied area. Weapon is unintentionally fired into an occupied area.	Persons struck by projectiles will be severely injured or perhaps killed. Objects struck may be damaged or destroyed.	Strict control of ranges to prevent presence of personnel in impact area. Instruction of all personnel in safe firearms handling and range safety procedures.	Reasonably probable	See TOP 3-2-504 for safety measures to be used on shoulder weapon test ranges.
1B	Same as above	Same as above	Weapon fires accidentally while sighted at an occupied area because	Same as above			
			1 Safety falls in safe position when trigger is pulled.		1. Conduct fault tree analysis to determine how safety can fall in safe position. Design weapon so that safety is fail-safe. Test prototype for failures.	Remote	1. See TOP 3-2-505 weapon test procedures.
			2 Weapon fires when cyclic rate selector is moved while safety is in safe position (automatic-semi-automatic weapons).		2. Conduct fault tree analysis to determine how safety can be affected by cyclic rate selector. Design weapon so that safety is independent of cyclic rate selector. Test prototype for failures.	Remote	2. See TOP 3-2-504 for weapon test procedures.
			3 Weapon fires when weapon is jarred with safety in fire position and trigger is not pulled		3. Conduct fault tree analysis to determine how firing pin can be jarred from cocked position. Design weapon so that firing pin cannot be jarred from cocked position.	Remote	3. See TOP 3-2-504 for weapon test procedures.

Figure 4-3. Example of a PHA Using Tabular Format

ysis (FMECA)—can be used to supplement the PHA as soon as sufficient design data become available. The limitation that becomes apparent in such cases in not the method of analysis itself but the level of data available and capability of the analyst to overcome this detracting factor.

For other purposes, such as establishing the safety baseline, the PHA is extremely beneficial. Within this framework, the analyst can develop the PHA to serve the needs of particular acquisition organizations, i.e., in the PHA he can point out the areas where lack of design data precludes conclusive results. This, in turn, will govern the additional types of analyses that may be required to complete the information. Determination of the purposes for which the PHA is to be used and of the information to be included depends on the analyst. He must be trained, experienced, and imaginative to be of most use in Army safety programs used in the acquisition process.

A factor affecting the efficiency and usefulness of the PHA concerns the time of its accomplishment. As indicated in Fig. 3-1, the probability that an error will be corrected is enhanced and the cost of correction reduced the earlier the error is detected. Conversely, any delay preventing the accomplishment of the PHA very early in the acquisition process can reduce its usefulness and effectiveness and lead to costly corrective action to achieve nonnegotiable safety requirements.

REFERENCES

1. MIL-STD 882B, *System Safety Program Requirements*, 30 March 1984.

2. DI-H-7048, *System Safety Hazard Analysis Report*, 1 May 1984.

3. TOP 3-2-504, *Safety Evaluation of Hand and Shoulder Weapons*, US Army Test and Evaluation Command, 1 March 1977.

APPENDIX 4A
INFORMATION SOURCES FOR SAFETY DATA AND RELIABILITY DATA

4A-1 INFORMATION SOURCES OF SAFETY DATA

SOURCE	INFORMATION AVAILABLE
US Army Safety Center Fort Rucker, AL 36362	Accident statistics
National Transportation Safety Board 800 Independence Avenue, SW Washington, DC 20594	Reports on transportation accidents
Defense Technical Information Center Building 5, Cameron Station 5010 Duke Street Alexandria, VA 22314	Reports and other information prepared by various Government and contractor activities
Department of Labor 200 Constitution Avenue Washington, DC 20210	Reports of industrial accidents
National Institute for Occupational Safety and Health Division of Safety Research Parklawn Building 5600 Fisher's Lane Rockville, MD 20857	Reports on analyses or experiments conducted to determine safe limits of exposure for personnel, hazardous characteristics of materials, and other safety problems involving people and their work environment
Consumer Product Safety Commission 1111 Eighteenth Street, NW Washington, DC 20270	Safety information, to include accident statistics, on consumer products
National Safety Council 444 North Michigan Avenue Chicago, IL 60611	Accident statistics derived from information submitted by members
Flight Safety Foundation 5510 Columbia Pike Arlington, VA 22204	Information on aircraft accidents, incidents, and design deficiencies
National Fire Protection Association 60 Batterymarch Street Boston, MA 02110	Statistics on fires and information on their avoidance. Issues fire codes and the National Electric Code
Manufacturing Chemists' Association, Inc. 1825 Connecticut Avenue, NW Washington, DC 20009	Statistics and accident description involving chemicals based on information submitted by its members. Provides information on hazardous chemicals, recommended equipment, materials, and handling procedures
Department of Defense Explosives Safety Board Room 856C, Hoffman Building Alexandria, VA 22331	Information on safety problems in the manufacture, testing, handling, transportation, and storage of ammunition

4A-2 INFORMATION SOURCES FOR RELIABILITY DATA

SOURCE	INFORMATION AVAILABLE
Reliability Analysis Center Rome Air Development Center Griffiss AFB, NY 13441	Reliability data on electronic and nonelectronic components of electronic systems
Chemical Propulsion Information Agency Applied Physics Laboratory Johns Hopkins University Baltimore, MD 21218	Data on liquid propellants and motors and other components for liquid propellant rocket motors; data on solid propellants and motors and other components for solid propellant rocket motors
Electronic Component Reliability Center and Mechanical Components Reliability Center Battelle Memorial Institute 505 King Avenue Columbus, OH 43201	Summaries of data from tests on electronic and mechanical parts
Interservice Data Exchange Program (IDEP) US Army IDEP Office US Army Missile Command Redstone Arsenal, AL 35809	Results of reliability tests on parts and statistical information

CHAPTER 5
SUBSYSTEM HAZARD ANALYSIS

The various methods of analysis used to develop a subsystem hazard analysis (SSHA) are discussed—i.e., failure mode and effects analysis (FMEA); failure mode, effects, and criticality analysis (FMECA); fault hazard analysis (FHA); fault tree analysis (FTA); and sneak circuit analysis (SCA). The techniques for performing these analyses, formats, data sources, examples, advantages, and limitations are presented.

5-0 LIST OF SYMBOLS

C_m = criticality number for failure mode, dimensionless

C_r = criticality number for item, dimensionless

CR = criticality ranking, dimensionless

F_R = ratio of occurrence of a specific failure mode, i.e., probability that part or item will fail in the identified mode, dimensionless

j = last failure mode in item under criticality classification, dimensionless

n = failure modes in items that fall under a particular criticality classification, dimensionless

P_L = probable damage resulting from a specific failure (by analysis or past data), dimensionless

Q = (1 − reliability) probability of component failure where reliability is obtained from tables or estimates from past data, dimensionless

t = duration of applicable mission phase usually expressed in hours or number of operational cycles, h or cycles

α = failure mode ratio, i.e., probability expressed as a decimal that part will fail in the identified mode, dimensionless

β = conditional probability expressed as a decimal that failure effect will result in identified criticality classification, dimensionless

λ_b = part base failure rate, h^{-1} or $cycles^{-1}$

λ_p = part failure rate, h^{-1} or $cycles^{-1}$

π_A = application factor that accounts for effect of application in terms of circuit function, dimensionless

π_E = environmental factor that accounts for influence of environmental factors other than temperature, dimensionless

π_Q = quality factor that accounts for effects of different quality levels, dimensionless

5-1 DESCRIPTION

An Army system is a machine or group of machines designed and built to perform a particular mission. For example, a particular type of tank or truck would constitute a system. The hazards associated with a system are frequently those related to the subsystems, assemblies, subassemblies, and components. The subsystem hazard analysis (SSHA) identifies hazards associated with the subsystem design including component failure modes, critical human error inputs, and hazards resulting from functional relationships among components and equipments comprising each subsystem (par. 203.1, Ref. 1). Subsequently, the hazards associated with the interface among subsystems are examined in the system hazard analysis (SHA) to identify safety problems for the system.

As a minimum, each subsystem must be examined. If a subsystem has been in use for sometime, it may be unnecessary for the analysis to go below the subsystem level since the hazards of the subsystem have been identified and corrective action taken. If a subsystem is new and has not had prior use, it may be necessary for the analysis to go to the component level.

The SSHA should be initiated as soon as the subsystems have been sufficiently defined to make the analysis possible. As the design matures and/or changes, the SSHA should be updated.

The results of the SSHA must be documented in some form, which will vary depending on the subsystem examined. Data Item Description (DID) DI-SAFT-80101 (Ref. 2) specifies the requirements for the SSHA report, i.e.,

1. Summary of the results
2. List of the identified hazards to include the information that follows:

a. *Component(s) Failure Mode(s)*. All failure modes that can result in a hazard are discussed. Generally, failure modes explain "how" something fails.

b. *System Event(s) Phase*. The mission phase that the system is in when the hazard is encountered is addressed.

c. *Hazard Description*. A complete description of the hazard is given.

d. *Effect on Subsystem and/or System*. The effect of the hazard on the subsystem must be considered. Also the possible upstream and downstream effects must be considered.

e. *Risk Assessment*. A risk assessment for each hazard, as defined in par. 4.5, MIL-STD-882 (Ref. 1) or as defined in other documents applicable to the system, will be given.

f. *Recommended Action.* The action that should be taken to eliminate or reduce the hazard is presented. Various courses of action should be discussed where appropriate. The recommended action(s) must be in sufficient detail to be of value to the design engineer.

g. *Effect of Recommended Action.* The change in the risk assessment that the recommended action will bring must be discussed.

h. *Remarks.* This block should be used for any information—such as references, administrative information, or data on previous, similar systems—that has not been included in other parts of the report.

i. *Status.* The status of action(s) to reduce or control the hazard must be given.

Various methods of analysis have been developed to obtain the information needed for the SSHA report. The methods described in this chapter are the failure mode, effects, and criticality analysis (FMECA); fault hazard analysis (FHA); fault tree analysis (FTA); and the sneak circuit analysis (SCA). These methods are used to identify and evaluate hazards that might exist in the individual subsystems and/or in elements of the subsystem. Through the use of these methods, the analyst can determine whether any element of the subsystem or the subsystem itself has any hazardous characteristics that require correction or removal. Also these methods can be used to determine whether any inadvertent operation, functional failure, or other malfunction could result in injury to personnel or damage to equipment.

5-2 ANALYSIS METHOD SELECTION

Before deciding on a specific analytical tool with which to conduct an SSHA, it is necessary to consider criteria related to the study and to establish pertinent guidelines once the analytical tool has been selected. These factors are discussed in the paragraphs that follow. A set of procedural steps for conducting an analysis also is presented.

5-2.1 CRITERIA

The normal criteria for the selection of the SSHA approach are to perform the analysis in the most cost-effective manner within applicable restraints. The principal restraints are budget and time span for performing the analysis and the design status of the equipment to be analyzed. Design status establishes the type of source data available to conduct a specific type of analysis. To minimize the cost of the analysis, the required detail and documentation should be no more than necessary to achieve the objectives. Principal guidelines follow (Ref. 3):

1. Specify quantitative results only to the extent essential.

2. Restrict the equipment indenture levels to be included in the analysis to the minimum number required.

3. Limit failure effects to those necessary to satisfy the purpose of the analysis.

4. Do not demand an analysis of all probable failure modes if an analysis of the principal failure modes will satisfy the purpose of the analysis—i.e., distinguish between what is desirable and what is necessary.

5. Restrict the use of FTA to very severe failure effects and to hazard analyses.

6. Limit documentation of the analysis to that essential to achieve its intended purpose.

5-2.2 BOUNDARIES AND LIMITS OF RESOLUTION

Failures can be considered at any level, i.e., down to individual parts and up to input and outputs of the item being analyzed. The greater the number of failure possibilities, i.e., the higher the level of detail, the greater will be the cost and time required for the analysis. Consider a TV set hooked up to cable. What constitutes the system to be investigated—the set itself, should the transmission cable be included, should the poles on which the cable is strung be included, what are the external boundaries of the system? Next, it is necessary to establish a limit of resolution, i.e., internal boundary. Consider the TV example. Will individual screws, knobs, and indicating lights be considered? It is obvious that the choice of appropriate system boundaries is important because the choice of external boundaries determines the comprehensiveness of the analysis, and the choice of a limit of resolution limits the detail of analysis. The life cycle phase of the system will dictate the various boundaries—a system in the concept stage would not require a detailed "nuts and bolts" analysis.

5-2.3 HARDWARE VERSUS FUNCTIONAL APPROACH

The SSHA can be conducted by using a hardware or functional approach. In the hardware approach, the effects of each failure mode are examined with respect to the function of the related individual hardware. The individual hardware effects are then related in sequence to the subsystem function.

In the functional approach, a detailed analysis is initiated by analyzing a system diagram of equipment functions rather than hardware items. This method is more adaptable to considering multiple failures and external influences such as human error. The functional approach is generally preferred when system definition has not matured to the point of identifying the specific hardware items that will perform the functions. This situation occurs in the early stages of development when hardware designs may not be completed and detailed item listings, system schematics, or assembly drawings may not be available. At a later stage of development, when system definition permits, equipment functions may be

replaced by their representative hardware items and a more detailed analysis performed, if necessary, using the hardware approach. Under certain circumstances a combined hardware-functional approach may be the optimum solution for conduct of the study.

5-2.4 PROCEDURAL STEPS

The method or approach adopted for performing an SSHA must be tailored to the subsystem under study; a universal cookbook procedure according to a fixed format or set of rules is neither logical nor appropriate. There are, however, general procedural steps that should be applied regardless of the particular analytic tool—FMECA, FHA, FTA, or SCA—selected. The procedural steps follow:

1. Define the system or hardware and its requirements.

2. Establish ground rules and assumptions for performing the analysis, e.g., define failure criteria.

3. Establish a block diagram or sequence of events.

4. Identify failure modes, effects, failure detection methods, and other worksheet requirements.

5. Evaluate the criticality of each failure mode.

6. Provide for the required corrective action and for evaluation of the adequacy of the corrective action.

7. Document the analysis and provide recommendations for those items that could not be corrected and the changes that should be imposed as maintenance requirements to insure that the inherent safety is achieved.

5-3 FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS

5-3.1 GENERAL

The failure mode, effects, and criticality analysis (FMECA) is defined by MIL-STD-1629 (Ref. 4) as essentially a reliability task; however, it supplements and supports other engineering tasks through the identification of areas—i.e., safety, readiness, mission success, maintenance, etc.—in which effort should be concentrated. Since the FMECA requires inputs from many disciplines, it is relatively unimportant which engineering group is selected to make the FMECA study. What is important is that a critical examination of the results, i.e., the potential design weaknesses that pose a safety problem, be made by safety engineers. Thus the FMECA becomes the point of departure for a detailed safety examination and recommended corrective actions.

The paragraphs that follow describe the FMECA technique in the broadest sense of usefulness.

5-3.2 DESCRIPTION AND PURPOSE

The purpose of the FMECA is to identify potential design weaknesses through systematic, documented consideration of (Ref. 5)

1. All likely ways in which a component or equipment can fail

2. Causes for each failure

3. Effects of each failure.

Although primarily a reliability tool (Ref. 5) to optimize performance and/or life cycle cost tradeoff between mission reliability and basic reliability at the black box, component, and/or system level, the FMECA is a powerful instrument for a detailed examination of subsystem safety. The FMECA features useful to the safety engineer are

1. Engineering schematics and mission rules that systematically identify the likely modes of failure

2. Possible effects of each failure, noting that each failure may be different for each phase of the life cycle or each type of mission

3. Criticality rating or number—usually based on failure effect, severity, and probability of frequency of occurrence—for each failure mode.

This latter feature, No. 3, distinguishes the FMECA from the failure mode and effects analysis (FMEA); the FMECA is a complementary analysis to the FMEA, i.e., its evolution is a two-stage process.

In essence, the FMECA lists the failure modes in an orderly, organized, evaluated manner; serves to verify design integrity and to identify and quantify sources of undesirable failure modes; and documents risks. The results of the analysis can be used to provide a rationale for changes in operating procedures for ameliorating the effects or for detecting the source of undesirable failure modes.

By applying the functional approach, an FMECA lends itself to the analysis of the subsystem in the concept exploration phase when specific items of hardware are still undetermined and only the more obvious failure modes can be identified. The analyses, if properly conducted, identify—by a schematic rearrangement—single failure points that may be eliminated. The FMECA must be updated periodically to keep pace with the maturity of the system.

Collateral benefits, derived from FMECA, that have related safety connotation are

1. Identification of critical items that are a part of selected configurations and should be retained and included in the request for proposal (RFP) for the full-scale development phase

2. Discovery of areas where judicious use of redundancy can significantly improve reliability and thus reduce the probability of occurrence of a hazard

3. Identification of areas that require environmental protection to improve safety

4. Evaluation of maintenance procedures using built-in test equipment (BITE), automatic test equipment (ATE), and other diagnostic tools.

The FMEA and the criticality analysis (CA), basic

elements of the FMECA, are discussed in the paragraphs that follow.

5-3.3 FAILURE MODE AND EFFECTS ANALYSIS

The FMEA, created after World War II as an engineering tool to improve hardware reliability, lends itself to a systematic approach that can be used for safety purposes, especially when accidents could result from hardware failures. The analysis, depending on system status, can employ a hardware or functional approach, discussed in pars. 5-3.3.2 and 5-3.3.3, respectively. The purposes, or objectives, of the approaches are the same; however, the techniques differ.

5-3.3.1 Failure Modes

For the purposes of the FMEA, the failure mode of the subsystem generally explains "how" it fails. Seven typical modes of possible equipment failure are (Ref. 4)
1. Premature operation
2. Failure to operate at a prescribed time
3. Intermittent operation
4. Loss of output, or failure, during operation
5. Degraded output or operational capability
6. Other unique failure conditions, as applicable, based on system characteristics and operational requirements or constraints
7. Failure to cease operation at a prescribed time.

In addition to the various failure modes previously enumerated, there are the additional descriptions of "how" or "in what manner" the failure occurred, which are of prime importance to the safety of the design. For example, a "single-point failure" is the failure of one item—e.g., a switch contact, the mechanical component of a solenoid, an electric wire, or any component or assembly, or an operator's error—that results in the single failure of the major item of which it is a part, and such failure is not compensated for through redundancy or an alternative operational procedure. From a safety viewpoint, no single-point failure should be acceptable in a design if it leads to unacceptable consequences. An alternative design should be chosen, even to prevent minor consequences, if the alternative is evaluated as cost-effective. Another example is a "common mode condition", i.e., the failure of one item that can lead to multiple consequences such as the failure of a cooling unit that causes the failure of all the electronic equipment that it cools. To determine whether a potential failure would be a single-point failure or a common mode failure, the safety analyst must have detailed knowledge of the subsystem design and its components together with their interrelationships.

It is important to note that the FMEA is concerned specifically with the failure to operate—the effects of a component, or larger item, on the operation of the subsys-tem. From the standpoint of system safety, however, many—perhaps most—of these failures are "safe" failures in that they cannot cause or contribute to accidents and thus are of no concern to the system safety engineer.

It is emphasized that the FMEA is a thorough examination of the strengths and weaknesses of a subsystem, i.e., a design tool. The FMEA is not a panacea for a poorly designed and/or operated subsystem.

5-3.3.2 Hardware Approach (Ref. 3)

The basic objective of the FMEA in this approach is to determine each possible mode of failure within an equipment and the effect of each mode of failure on the overall subsystem or portion thereof. A detailed analysis using this approach is begun by tabulating each individual equipment item and then analyzing it. Failure effects on performance of the item itself and on other hardware subsystem elements are then determined and become failure modes at the next higher indenture level. The hardware approach is more rigorous than the functional approach and normally is used whenever hardware items can be identified from engineering drawings. Usually the hardware approach is used from the part level up; however, it can be initiated at any indenture level and progress in either direction.

5-3.3.3 Functional Approach (Ref. 3)

The functional approach is initiated by listing equipment functions at an initial indenture level. Failure modes contributing to nonconformance levels of the desired functions are then analyzed and failure effects are determined, which then become the failure modes at the next lower indenture level. The procedure is continued down or up to indenture levels, as determined by the analysis, to identify all critical items. This approach normally is used for those cases in which hardware system definition has not reached the point of identifying specific hardware items or in those situations in which the complexity of the hardware system is such that an analysis from the initial indenture level down is the more practical procedure to follow. The functional approach, obviously, is not as cumbersome and difficult to follow as the hardware approach. Although the functional approach normally is applied from an initial level down, it can be initiated at any indenture level and progress in either direction.

5-3.4 CRITICALITY ANALYSIS

"Criticality" and "safety critical" are similar, but not necessarily identical, terms. Safety critical—an important factor in other aspects of system safety—refers to a unit of equipment or an operating procedure whose failure to perform as intended will endanger personnel and/or materiel because of the hazardous consequences. Performing as intended includes the reliability of the unit and the probability that prescribed operating procedures will

be observed. A unit of equipment or an operating procedure can have a low level of reliability and a low probability that the specified procedures will be observed, however, without necessarily resulting in a safety-critical condition. It is only when the consequences will be unacceptable from a safety viewpoint that low reliability and low probability will generate a safety-critical situation.

Criticality—the factor relating to the FMECA—is a relative term used to measure, from a reliability viewpoint, the consequences of a hardware failure. Safety is a factor to be considered, but of direct importance is the loss of operational capability that might be perfectly acceptable from a safety viewpoint.

5-3.4.1 Criticality versus Severity

In the CA, each potential failure mode identified in the FMEA—based on the best available data—is ranked according to the combined influence of the severity classification and the probability of occurrence (Ref. 5). Criticality rankings in the FMECA attempt to indicate, in a numerical scheme, the consequences of component failure. Criticality rankings are desirable to determine

1. Which items should be given more intensive study for the elimination of a hazard that could cause the failure; and for fail-safe design, failure rate reduction, or damage containment

2. Which items require special attention during production, require rigid quality control, and require protective handling at all times (critical-item list)

3. Special requirements to be included in specifications to suppliers

4. Acceptance standards to be established for components obtained from subcontractors and for parameters of subcontract items that should be tested intensively

5. When special procedures, safeguards, protective equipment, monitoring devices, or warning systems should be provided

6. Where accident prevention efforts and funds could be applied most effectively.

It is important to remember that although reliability techniques and data are used in the system safety analysis, there are certain reliability terms that sound similar to safety terms but have different definitions. In the present discussion "criticality ranking" is not necessarily identical to "hazard severity" or to "hazard probability ranking". The primary purpose of criticality ranking is to identify parts, assemblies, or components that are critical to the continued operation of the equipment in a manner that ranks them in relative importance. In effect, the criticality ranking can assist in a safety analysis in that it is, in part, an assignment of numerical factors to each of the terms "hazard severity" and "hazard probability". This result is then combined with additional refinements to account for factors such as (1) how each part fails in order to achieve the specific consequences of that failure and (2) whether

there is sufficient time after the initial failure to stop the chain reaction due to such failures and continue operations. A part could receive a high criticality ranking without affecting system safety.

On the other hand, the "hazard severity" and "hazard probability" definitions of Ref. 1 are qualitative measures of the effects upon the safety consequences of a failure. Thus the CA combines severity with both the probability and the frequency of occurrence. "Hazard severity" and "hazard probability" are discussed in pars. 5-3.4.2 and 5-3.4.3, respectively.

5-3.4.2 Hazard Severity (Ref. 1)

"Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem, or component failure or malfunction as follows:

Description	Category	Mishap Definition
Catastrophic	I	Death or system loss
Critical	II	Severe illness, severe occupational illness, and major system damage
Marginal	III	Minor illness, minor occupational illness, or minor system damage
Negligible	IV	Less than minor injury, occupational illness, or system damage.

The hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the MA [managing activity] and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness."

In evaluating the criticality of a failure mode, the following factors should be taken into account (Ref. 3):

1. *Monitorability.* A measure of confidence in being able to detect—and to act upon detection—that the failure has occurred.

2. *Exposure Time.** The period of time since the subsystem was known to be good. If the failure is critical for a specific phase of the operation but is also monitorable, the exposure time for that phase should be considered.

---

*Exposure time is the period in clock time, or cycles, during which an item is exposed to failure measured from when it was last functioning to when it is verified again.

3. *Probability.* Given that a failure is undetectable, or only monitorable under certain conditions, its resulting exposure time may be significant. The probability should be considered that other specific failures may combine within the defined exposure time, in the aggregate, in a critical failure effect. At some point the failure combinations may become so improbable that the failure need no longer be considered. The requirement for "how improbable" must necessarily be a function of the application.

5-3.4.3 Hazard Probability (Ref. 1)

"The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is:

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely it can be assumed occurrence may not be experienced.	Unlikely to occur but possible

---

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

Although these terms from Ref. 1 as defined are qualitative in nature, a system of numbers can be assigned to them for generating a type of criticality number. It is probably better to consider other factors, too—as previously mentioned—rather than making a decision based on assigned severity and probability numbers alone.

5-3.4.4 Quantitative Technique

An example of the extreme in determining criticality rankings is described in Ref. 3, which requires the solution of an equation with six factors for each failure mode and then integration of the results for all failure modes. A preferable method is a simpler one described in Ref. 6. It uses the relationship

$$CR = P_L \times Q \times F_R, \text{dimensionless} \quad (5-1)$$

where
CR = criticality ranking, dimensionless

P_L = probable damage resulting from a specific failure mode (by analysis or past data), dimensionless

Q = (1 − reliability) probability of component failure where reliability is obtained from tables or estimates from past data, dimensionless

F_R = ratio of occurrence of a specific failure mode, i.e., probability that part or item will fail in the identified mode, dimensionless.

An alternate number system is the Criticality Classification Code proposed by Arnzen (Ref. 7). The system consists of three independent categories that indicate
   1. P = probability of occurrence
   2. T = reaction time criticality
   3. C = consequences of failure if not compensated for.
Each of these three categories is ranked as follows:
   P, the probability of occurrence:
      1 = highly likely
      2 = likely
      3 = not likely
   T, the reaction time criticality (relative to correction of the failure to prevent unwanted consequences):
      1 = reaction time critical
      2 = reaction time limited
      3 = reaction time unlimited
   C, the consequence of failure:
      1 = uncompensated effect is catastrophic
      2 = may be critical for mission success if not compensated
      3 = no major consequence to mission success or crew safety.
Examples of the application and interpretation of this three-part criticality ranking follow:
   1. 1-1-1 (corresponding to the rankings assigned to categories (P-T-C-)) indicates failure is highly likely, action must be taken immediately, otherwise the crew will be lost.
   2. 3-2-3 indicates failure is not likely, no need to take immediate action, and the failure will not hamper mission success or crew safety.

Another method of ranking criticality is to multiply the failure severity level number by the failure probability level number. In this instance, the reliability numbers from tables, tests, or past history of similar parts are used to obtain a probability number. Bands of reliability numbers in the areas of interest are assigned probability numbers. The severity level numbers are based on failure consequences—including operational considerations, partial failures versus complete failures—and whether the failures affect safety of personnel and equipment. The result of the multiplication is the criticality number. An example of this technique is given in par. 5-3.7.

5-3.4.5 Qualitative Technique

The availability of specific parts configuration data and failure rate data will indicate the best analysis approach to use for a particular criticality analysis. In par. 5-3.4.4 quantitative approaches were discussed. The qualitative approach is appropriate when specific failure rate data are not available. When the failure probability levels are used in this approach, they should be modified as the subsystem design matures and becomes better defined. Also when parts configuration data and failure rate data become available, criticality numbers should be calculated and incorporated in the analysis.

To progress in the absence of failure rate data, assess the failure modes identified in the FMEA in terms of probability of occurrence levels defined in the paragraph that follows. Individual failure mode probabilities of occurrence should be grouped into distinct, logically defined levels that establish the qualitative failure probability level for entry into the appropriate CA worksheet column.

A suggested technique for defining probability of occurrence levels, excerpted from Ref. 4, follows: (Note that the basic definitions of probability levels follow those for hazard probability in MIL-STD-882 (Ref. 1).)

1. "*Level A—Frequent*. A high probability of occurrence during the item operating time interval. High probability may be defined as a single failure mode probability greater than 0.20 of the overall probability of failure during the item operating time interval."

2. "*Level B—Reasonably Probable*. A moderate probability of occurrence during the item operating time interval. Probable may be defined as a single failure mode probability of occurrence that is more than 0.10 but less than 0.20 of the overall probability of failure during the item operating time."

3. "*Level C—Occasional*. An occasional probability of occurrence during item operating time interval. Occasional probability may be defined as a single failure mode probability of occurrence that is more than 0.01 but less than 0.10 of the overall probability of failure during the item operating time."

4. "*Level D—Remote*. An unlikely probability of occurrence during item operating time interval. Remote probability may be defined as a single failure mode probability that is more than 0.001 but less than 0.01 of the overall probability of failure during the item operating time."

5. "*Level E—Extremely Unlikely*. A failure whose probability of occurrence is essentially zero during item operating time interval. Extremely unlikely may be defined as a single failure mode probability of occurrence that is less than 0.001 of the overall probability of failure during the item operating time."

The entries given in the example of Fig. 5-5 illustrate that the objective of reliability engineering is to discover where to place the most emphasis to obtain reliable equipment—first in an operational sense and secondarily in a safety sense. The entries illustrate that there is no constant relationship between the reliability criticality numbers and the safety categories as defined in MIL-STD-882 (Ref. 1). Another sheet from this same analysis (not shown in Fig. 5-5) contains an entry with a reliability criticality number of 12, which requires corrective action (according to reliability guidance), but a safety category of IV (negligible). This is understandable because the reliability criticality number is designed for use only in rating the hardware. Personnel errors, whether induced by a poor design or unavoidable design requirements, can cause Category I hazard severity consequences even though the hardware itself may have a very low reliability criticality number or failure rate.

Though the foregoing comments are somewhat negative regarding the direct correlation of the criticality number with safety, the criticality column of the FMECA does serve useful safety purposes. The higher numbers should indicate areas of the design to be subjected subsequently to more detailed analysis. In addition, these higher criticality numbers—for reliability engineering purposes any criticality number over 10 indicates a required change—will provide clues as to the priorities for design changes that can affect safety. In toto, the complete FMECA report provides much data, in addition to criticality numbers, that can be used in safety analyses.

5-3.5 ANALYSIS TECHNIQUE AND FORMAT

Prior discussions have recommended a degree of flexibility in adapting various techniques to individual safety analyses. The approach for the FMECA will also be somewhat flexible depending on the point in the system development program at which this analysis is undertaken.

5-3.5.1 Technique

The exact procedure to follow for accomplishment of the FMECA still depends on various factors such as the point in the system development program at which the

analysis is made, the complexity of the item to be analyzed, and the depth to which the analysis can or should proceed. Two approaches can be used: (1) the functional approach—when individual parts or items to be incorporated in the subsystem have not yet been identified (see par. 5-3.3.3) and (2) the hardware approach—when the parts and comments can be identified from engineering drawings (see par. 5-3.3.2). Both approaches use the same general procedures. The first part of an FMECA is the development of an FMEA, a process described in par. 5-3.5.1.1.

5-3.5.1.1 Performing the FMEA

The FMEA is usually prepared by reliability engineering personnel. Occasionally, however, contract provisions will require that it be done by system safety personnel. Regardless of the preparing activity the following discrete steps are to be used in performing an FMEA in preparation for the FMECA (Ref. 4):

1. *Define the Subsystem to be Analyzed.* Complete subsystem definition includes identification of internal and interface functions, expected performance at all indenture levels, subsystem restraints, and failure definitions. Functional narratives of the subsystem should include descriptions of each mission—in terms of functions that identify tasks to be performed for each mission, mission phase, and operational mode. These narratives should describe the environmental profiles, expected mission times and equipment use, and the functions and outputs of each item.

2. *Construct Block Diagrams.* Functional and reliability block diagrams should be obtained or constructed for each item involved in the use of the subsystem to illustrate its operation, interrelationships, and interdependencies. All subsystem interfaces shall be indicated. (If the hardware approach is being used, "item" refers to assembly, subassembly, or component—depending upon the level of detail undertaken. If the functional approach is being used, then "item" refers to function.)

3. Identify all potential failure modes for the item and its interfaces, and define their effects on the immediate function or item, on the subsystem, and on the mission to be performed.

4. Evaluate each failure mode in terms of the worst potential consequences that may result, and assign a severity classification category in accordance with the definitions in MIL-STD-882 (Ref. 1). (Severity categories are given in par. 5-3.4.2.)

5. Identify failure detection methods and compensating provisions for each failure mode.

6. Identify corrective design or other actions required to eliminate the failure or to control the risk.

7. Identify the effects or other subsystem attributes of those corrective actions, such as changed requirements for logistic support.

8. Document the analysis, summarize the problems that could not be corrected by design, and identify the special controls that are necessary to reduce failure risk. This completes the FMEA.

5-3.5.1.2 Criticality Analysis Process (Ref. 4)
5-3.5.1.2.1 Calculation of C_m

The CA process involves calculating the value of the criticality number C_m for each *failure mode* determined in the FMEA process. The C_m is the portion of the criticality number for the item due to one of its failure modes under a particular severity category. For a particular severity category and operational phase, the C_m for a failure mode may be calculated by

$$C_m = \beta \alpha \lambda_p t, \text{ dimensionless} \qquad (5\text{-}2)$$

where

C_m = criticality number for failure mode, dimensionless

β = conditional probability expressed as a decimal that failure effect will result in identified criticality classification, dimensionless

α = failure mode ratio, i.e., probability expressed as a decimal that part will fail in identified mode, dimensionless

λ_p = part failure rate, h^{-1} or cycles^{-1}

t = duration of applicable mission phase usually expressed in hours or number of operation cycles, h or cycles.

5-3.5.1.2.2 Calculation of C_r

The second criticality number calculation is for the *item* under analysis. The criticality number C_r for an item is determined by the number of subsystem failures of a specific type expected due to the failure modes of the item. The specific type of subsystem failure is expressed by the severity category for the failure modes of the item. For a particular severity category and mission phase, the C_r for an item is the sum of the failure mode criticality numbers C_m under the particular severity category. C_r is calculated by

$$C_r = \sum_{n=1}^{j} (\beta \alpha \lambda_p t)_n, n = 1, 2, 3, ..., j, \text{ dimensionless}$$
$$(5\text{-}3)$$

i.e., a summation of failure modes C_m for the items that fall under a particular criticality classification,
where

C_r = criticality number for item, dimensionless

n = failure modes in items that fall under a particular criticality classification, dimensionless

j = last failure mode in item under criticality classification, dimensionless

β = conditional probability expressed as a decimal that failure effect will result in identified criticality classification, given that the failure mode occurs, dimensionless. The β values represent the analyst's judgment as to the conditional probability the loss will occur and should be quantified in general accordance with the following:

Failure Effect	β Value
Actual loss	$\beta = 1.00$
Probable loss	$0.10 < \beta < 1.00$
Possible loss	$0 < \beta \leq 0.10$
No effect	$\beta = 0$

α = failure mode ratio, probability expressed as a decimal, that part or item will fail in the identified mode, dimensionless. The fraction of the part failure rate λ_p related to the particular failure mode under consideration shall be evaluated by the analyst and recorded. If all potential failure modes of a particular part or item are listed, the sum of the α values for that part or item will equal unity. Individual failure mode multipliers may be derived from failure rate source data or from test and operational data. If failure mode data are not available, the α values shall represent the analyst's judgment based upon an analysis of the functions of the item.

5-3.5.1.2.3 Criticality Matrix

A criticality matrix will then be prepared to provide a means of identifying and comparing each failure mode to all other failure modes with respect to severity. The matrix is constructed by inserting item or failure mode identification numbers in matrix locations representing the severity classification category and either the probability of occurrence level or the criticality number C_r for the failure modes of the item. The resulting matrix display shows the distribution of criticality of the failure modes of the item and provides a tool for assigning corrective action priorities.

5-3.5.2 Format

Formats for the FMEA, CA, and CA matrix are presented in Figs. 5-1, 5-2, and 5-3, respectively.

5-3.6 SOURCES OF RELIABILITY DATA

Failure rate and failure rate adjustment factor data, e.g., environmental and quality factors, for the FMEA are available from many sources. MIL-HDBK-217 (Ref. 8) is the primary source of failure rate data for electronic parts. Both the base failure rate and all failure rate adjustment factors should be identified. When parts are similar to those listed in MIL-HDBK-217, base failure rates should be selected from MIL-HDBK-217 and should include other adjustment factors—such as special quality factors, application factors, and environmental factors—as may be required to modify the MIL-HDBK-217 data for applicability to the particular part.

Failure rate data for parts not covered by MIL-HDBK-217 should be selected from alternative data sources; Ref. 9 is a data source for nonelectronic parts. Other sources of data are listed in par. 4A-2, Appendix 4A.

Data on failures and their consequences in a specific system generally can be obtained from the Army commodity command responsible for that system or from the contractor from which it was acquired. Field reports of deficiencies, submitted because components or assemblies caused, or were involved in, operational accidents, can provide valuable insights into potential safety problems that result from failures. These deficiency reports are

1. Army Safety Management Information System (ASMIS)
2. Quality deficiency report (QDR)
3. Sample data collection (SDC)
4. Equipment improvement report (EIR).

Parts common to fielded materiel and the materiel being developed give clues to potential safety problems of the new design. Even though part or item commonality cannot be established, existing systems with functions similar to new systems can provide helpful insight as to where potential safety problems might be found in the new design. New technology may enable the elimination of the previous safety deficiencies, and this information should be documented in the hazard analyses of the subsystem.

5-3.7 EXAMPLES

To illustrate the FMEA and CA, examples from Army materiel development programs are provided. These are given in Figs. 5-4 and 5-5, respectively.

5-3.7.1 FMEA Example

Fig. 5-1 illustrated the format for an FMEA worksheet. The word "worksheet" emphasizes the point that the FMEA is a working step toward preparation of the FMECA. A completed example of the FMEA worksheet is given in Fig. 5-4.

FAILURE MODE AND EFFECTS ANALYSIS

SYSTEM _____
SUBSYSTEM _____
INDENTURE LEVEL _____
REFERENCE DRAWING _____
MISSION _____

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE OPERATIONAL MODE	FAILURE EFFECTS			FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	MIL-STD-882 SEVERITY CLASS	REMARKS
					LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

Figure 5-1.   Example of FMEA Worksheet Format (Ref. 4)

CRITICALITY ANALYSIS

SYSTEM _____
SUBSYSTEM _____
INDENTURE LEVEL _____
REFERENCE DRAWING _____
MISSION _____

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS MIL-STD-882	FAILURE PROBABILITY / FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY β	FAILURE MODE RATIO α	FAILURE RATE (PART) λ_p	OPERATING TIME t	FAILURE MODE CRIT NO $C_m = \beta\alpha\lambda_p t$	ITEM CRIT NO $C = \sum_{i}^{n}(c_m)$	REMARKS

Figure 5-2.   Example of CA Worksheet Format (Ref. 4)
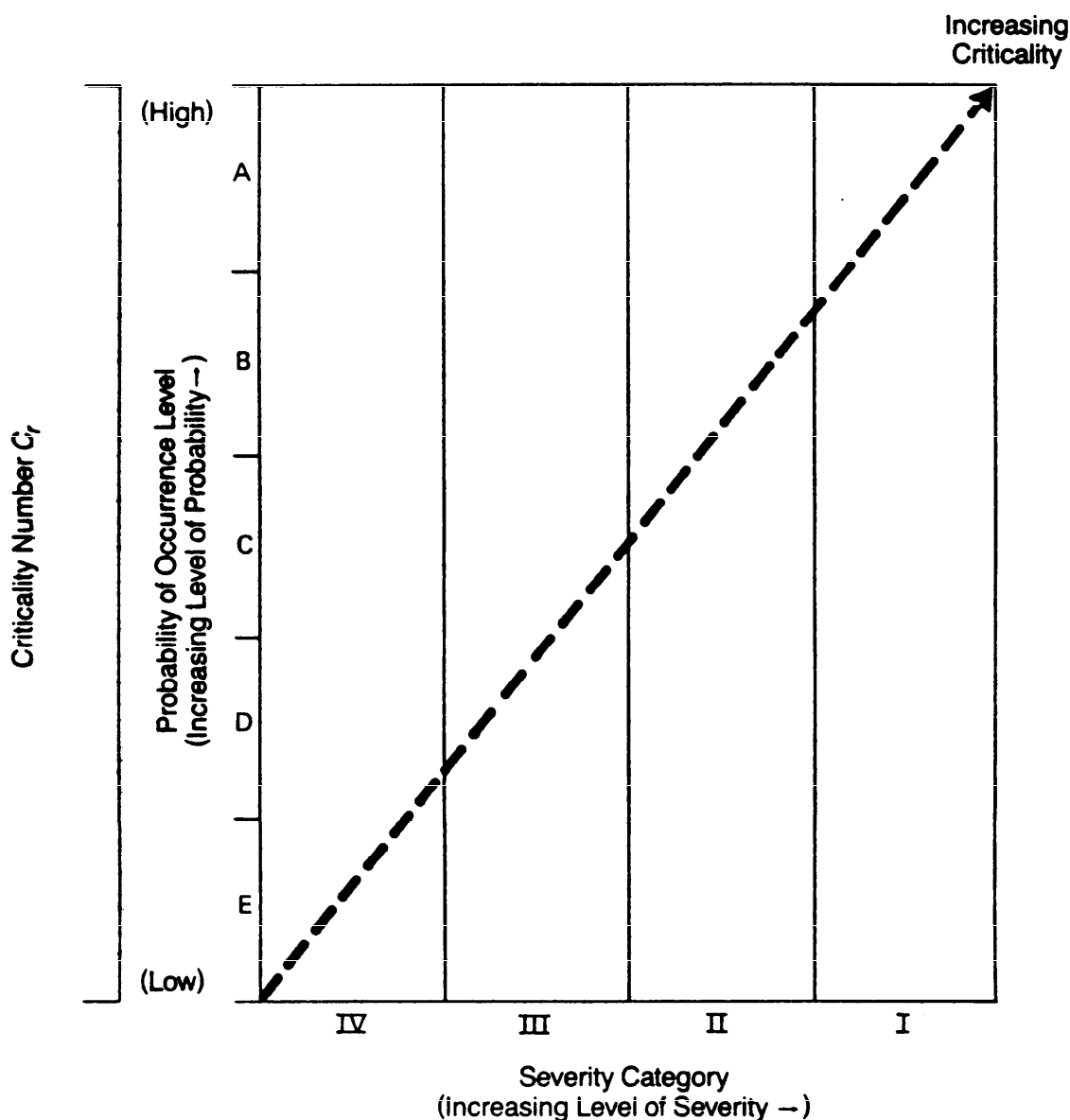
Figure 5-3. Format for Criticality Matrix (Ref. 4)

5-3.7.2 FMECA Example

The example of an FMECA presented in Fig. 5-5 is a page from an analysis of a subsystem in the Army's Bradley Infantry Fighting Vehicle System (IFVS). The original report page has been modified for use in this handbook. The analysis was made during the full-scale development phase of system acquisition, and, though originally titled "Failure Mode and Effects Analysis", the content of the table includes criticality information. This would, more properly, make it a "Failure Mode, Effects, and Criticality Analysis"; therefore, it is used here as an example of an FMECA.

An example of calculating the critical numbers C_m and C_r for a given mission phase under a severity classification

Category II follows. The values of the base failure rate λ_b and factors π_i that modify λ_b for the category of environmental applications and other factors that affect part reliability—together with the method—were taken from MIL-HDBK-217 (Ref. 8). The item under analysis is a diode, Group V, MIL-S-19500/533 (Ref. 10), used as voltage reference in a fixed ground environment at 25°C and of a Joint Army and Navy (JAN) quality level. Given:

$\lambda_b = 0.00053 \times 10^{-6}$/h, part base failure rate

$\pi_A = 1.5$, application factor that accounts for effect of application in terms of circuit function, dimensionless

SYSTEM _____
SUBSYSTEM _____
INDENTURE LEVEL _____
REFERENCE DRAWING _____
MISSION _____

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS MIL-STD-882?	FAILURE PROBABILITY / FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY β	FAILURE MODE RATIO α	FAILURE RATE (PART) λ_p	OPERATING TIME t, h	REMARKS
	Browpad Assembly	Steady Operator's Head	Soft Material Gouged or Torn	Targeting, Missile Launch and Guidance During Flight	II	Manufacturer's Field Experience	0.5	1	1.04×10^{-6}	1	
	Headrest Eyepiece	Reduce Operator Strain	Broken		III	Data From Using Commands	0.5	1	0.001	1	
	Handle Browpad	Permit Adjustments	Broken		IV		0.5	1	0.092	1	
	Retainer Browpad	Holds Browpad in Position	Detaches From Headrest		III		0.5	1	0.001	1	
	Support Browpad	Holds Browpad in Position	Breaks		II		0.5	1	0.3	1	
	Spring	Locks Browpad in Position	Breaks		IV		0.5	1	0.3	1	
	Pin, Spring	Holds Spring in Place	Falls Out of Hole		IV		0.5	1	0.001	1	

Figure 5-4. Failure Mode and Effects Analysis

CRITICALITY ANALYSIS

SYSTEM _Infantry Fighting Vehicle System (IFVS)_
SUBSYSTEM _TOW Weapon System_
INDENTURE LEVEL _Part_
REFERENCE DRAWING _75-168 L1A_
MISSION _Targeting for Missile Launch_

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS MIL-STD-882	FAILURE PROBABILITY/ FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY β	FAILURE MODE RATIO α	FAILURE RATE (PART) λ_p	OPERATING TIME t	FAILURE MODE CRIT. NO. $C_m = \beta \alpha \lambda_p t$	ITEM CRIT. NO. $C_r = \sum_{1}^{j} (c_m)$	REMARKS
	Bumpad Assembly	Steady Operator's Head			II	Manufacturer's Field Experience	0.5	—	1.04×10^{-4}	—	0.52	0.8675	
	Headrest Cupper	Reduce Operator Strain	Soft Material Gouged or Torn	Targeting, Missile Launch and Guidance During Flight	III	Data From Using Commands	0.5	—	0.001	—	0.0005		
	Handle Bumpad	Permit Adjustments	Broken		IV		0.5	—	0.092	—	0.046		
	Retainer Bumpad	Holds Bumpad in Position	Detaches From Headrest		III		0.5	—	0.001	—	0.005		
	Support Bumpad	Holds Bumpad in Position	Breaks		II		0.5	—	0.3	—	0.15		
	Spring	Locks Bumpad in Position	Breaks		IV		0.5	—	0.3	—	0.15		
	Pin Spring	Holds Spring in Place	Falls Out of Hole		IV		0.5	—	0.001	—	0.0005		

Figure 5-5. Criticality Analysis

$\pi_E = 3.9$, environmental factor that accounts for influence of environmental factors other than temperature, dimensionless

$\pi_Q = 3.0$, quality factor that accounts for effects of different quality levels, dimensionless.

Solve for the part failure rate λ_p by (Ref. 8)

$$\lambda_p = \lambda_b(\pi_A\pi_E\pi_Q), \text{ failures}/\text{h} \qquad (5\text{-}4)$$
$$= 0.00053\times10^{-6} \, (1.5 \times 3.9 \times 3)$$
$$= 0.00930\times10^{-6} \text{ failures}/\text{h}.$$

For this specific mission phase there are two failure modes under severity classification Category II and one failure mode under severity Category IV. The fraction α_i of the part failure rate λ_p related to the particular failure rate under consideration is

$\alpha_1 = 0.3$ for first failure mode under severity Category II

$\alpha_2 = 0.2$ for second failure mode under severity Category II

$\alpha_3 = 0.5$ for failure mode under severity Category IV. (Note that $\Sigma\alpha_i = 1$.)

Assume the conditional probability of mission loss $\beta = 0.5$ and $t = 1$h for the mission phase. Therefore, C_m from Eq. 5-2 is

1. *For $\alpha_1 = 0.3$:*
   $C_m = (0.5)(0.3)(0.00930\times10^{-6}) = 0.001395\times10^{-6}$

2. *For $\alpha_2 = 0.2$:*
   $C_m = (0.5)(0.2)(0.00930\times10^{-6})(1) = 0.000930\times10^{-6}$

Since by Eq. 5-3

$$C_r = \sum_{n=1}^{2} (C_m)_n$$
$$= 0.001395\times10^{-6} + 0.000930\times10^{-6}$$
$$= 0.002325\times10^{-6}$$

under severity Category II. The $\alpha_3 = 0.5$ case was not considered because α_3 related to a Category IV severity.

5-3.8 ADVANTAGES

The subsystem FMEA and FMECA reports provide both qualitative and quantitative data useful in completing other safety analyses and special safety studies. The qualitative part of these reports identifies items in the subsystem, their failure modes, and the effects of these failure modes on other items and the subsystem. The safety analyst can use these data to investigate safety

effects in more detail, including the human interfaces of these failures. Investigation of some failure modes will identify the need to develop safe maintenance procedures. If safe maintenance procedures cannot be developed to correct a particular failure, the analyst will request a design change for safety reasons. Thus the qualitative analysis can avoid costly modifications by ferreting out latent design and operational deficiencies in the early design and testing phases of subsystem development to insure a high level of safety before the initiation of production.

The quantitative portion of the FMEA and FMECA analyses provides the basic numerical data to calculate probability levels for safety level determination. Remember that not every line of the FMEA and FMECA will be a safety problem. Some failure modes are "fail inoperate" and are safe; but to the extent failure rates are provided, they can be used in special safety studies or other hazard analyses as appropriate to the safety process. The high criticality numbers provide useful clues both to items that should be studied to identify possible hazards and to the relative priorities for design changes to eliminate these hazards.

5-3.9 LIMITATIONS

The principal factors that limit the use of the FMECA for safety purposes are

1. It is generally economically unjustifiable to analyze every part, item, or component of a subsystem in an FMECA for safety purposes. Only a few of the components in the subsystem may cause accidents if they fail and thus be of concern to the safety analyst.

2. FMECAs generally are concerned only with individual failures and their downstream effects. Conditional failures, i.e., those brought about by other factors such as environment, and multiple failures may not be considered in the FMEA or FMECA analysis.

3. Equipment malfunctions (failures) are only one source of hazards that can lead to accidents. The FMEA and FMECA contain no information on hazardous characteristics of components or subsystems, none on operator errors, and little on effects of adverse environments. The FMEA and FMECA can, therefore, be used to identify only those potential accidents that could result from component or subsystem malfunctions.

5-4 FAULT HAZARD ANALYSIS
5-4.1 PURPOSE AND DESCRIPTION

The fault hazard analysis (FHA) is a detailed investigation of a subsystem to determine component hazard modes, causes of those hazards, and the resultant effects to the subsystem and its operation (Ref. 1).

The FHA was developed shortly after the advent of the system safety programs in an effort to correct the principal shortcomings of the FMEA and FMECA for safety

analysis purposes. Both the FMEA and FMECA consider only potential failures; they do not consider human error resulting from particular hardware designs, hazardous conditions, or adverse environmental effects. On the other hand, the FHA considers those areas not considered by the FMEA or FMECA.

The FHA is generally a qualitative analysis; it usually does not include quantitative probabilities. The major reasons for this are that probability data on hazardous characteristics and environmental effects that are considered in the FHA are difficult or impossible to obtain and data on operator errors are available only occasionally and then only to a limited extent.

As stated, an FHA is conducted to address not only malfunctions but also human error, hazardous characteristics, and adverse environmental effects. To address these elements, the FHA will include

1. All subsystem faults resulting from component failures, hazardous subsystem operating characteristics, adverse environmental conditions, and any related human operator or maintenance error that could lead to accidents

2. The potential effects of the faults, the means by which occurrence of the faults can be minimized, and the safeguards with which their adverse effects could be controlled or eliminated

3. The upstream conditions and events that could create or contribute to the occurrence of the faults.

FHA has not been widely used because of the expanded use of other analysis techniques and the development of newer ones. Nevertheless, the FHA does have its uses; therefore, it is included as an analysis technique for performing the SSHA. The FHA is used for subsystem hazard analyses in which malfunctions will be the principal cause of accidents. Also it is used as an adjunct to other analyses such as the fault tree analysis. As a diagnostic tool, the FHA is superior to a preliminary hazard analysis (PHA) because it provides more detailed and updated information on potential failures of specific subsystems and components. The FHA follows the PHA and, therefore, it is an extension, rather than a duplication, of the PHA.

5-4.2 ANALYSIS TECHNIQUE AND FORMAT

In constructing the FHA, the safety analyst relies heavily upon data from the FMEA, which indicates that a hazard would result from a failure. In those system development programs not requiring an FMEA, the analyst must undertake a complete review of the subsystems and components of the subsystem to establish where faults due to failures could result in injury or damage.

5-4.2.1 Technique

Regardless of the type of background data used in the FHA, the analyst must be inquisitive as to how the sub-

system and its components can have hazardous characteristics, be commanded to perform in a hazardous mode through personnel error, or revert to a hazardous mode through environmental influence.

To prepare a fault hazard analysis, the analyst should

1. Determine how the system is to operate and the functions of all the constituent subsystems and components.

2. Determine the potential injury or equipment damage that could result from the failure of a specific component and when in the operation of a subsystem this problem could occur.

3. Evaluate the potential causes of the fault—i.e., whether it is a failure of the component itself under normal operating conditions or whether it is a "commanded" fault due to an upstream event that overloaded the component, circuit, or subsystem.

4. Identify and evaluate the upstream events that could "command" a fault.

5. Identify and evaluate the downstream effects that could result from the failure of a component, circuit, or subsystem and would cause injury or damage.

6. List the measures that would minimize or reduce faults or the effects that the faults could generate.

5-4.2.2 Format

The format for an FHA is a function of the particular subsystem being analyzed. Thus the column headings for the FHA should be tailored to satisfy the requirements of the particular item being analyzed.

Since the information from an FHA is used to provide inputs to the SSHA report described in DID DI-SAFT-80101 (Ref. 2), the information required by the DID preparation instructions can be put into an FHA tabular format with column headings that match the data required by the DID. This information is almost the same as that required by the DID for a PHA. One of the few differences is a column title change of "Effect on System" for the PHA to "Effect on Subsystem" for the FHA. In addition, the FHA format should contain columns for information on the upstream and downstream effects; these columns have special significance for the fault tree analyst. Fig. 5-6 (Ref. 11) is a functional type of FHA format that is simplified so variations of each column can be easily made to satisfy any development program. An example of how Fig. 5-6 can be altered to accommodate a specific subassembly is illustrated by Fig. 5-7.

5-4.3 SOURCES OF DATA

Because of its similarity to the PHA, data for the conduct of an FHA can be obtained from the same sources. Design engineers also can assist the safety analyst in understanding the manner in which the system and subsystems operate and the functions of all subsystem components. In addition, field reports submitted to Army

Item, Event, or Condition	What is the Potential Problem?	Why Can It be a Problem?	Will it Cause Downstream Damage?	What Upstream Input or Component can "Command" the Un-desirable Event?	Compensation or Control?	Remarks

Willie Hammer, PRODUCT SAFETY MANAGEMENT AND ENGINEERING, ©1980. p. 183. Reprinted by permission of Prentice-Hall, Inc., Englewood Cliffs, NJ.

Figure 5-6.   Simplified Column Headings for Fault Hazard Analysis (Ref. 11)

Major Component	Component Failure Mode	Component Failure Rate (Primary)	System Operational Mode	Effect of Primary Component Failure on Subsystem	Factors that Cause Secondary Component Failure	Upstream Components or Inputs That may "Command" the Undesired State	Hazard Classification	Remarks
Battery	No Output	N/A	Pumping/Standby	No Power to Fuse	Low External Load; High Mechanical Shock	Personnel Error	Safe	
	Leakage	N/A	Pumping/Standby	Corrosion in Battery Area	High Mechanical Shock	Personnel Error	Marginal	
Fuse	Short	N/A	Pumping/Standby	Power Circuit Complete to Power Relay 2 Contacts	Low Thermal Environment	A. Fused Oversize; B. Replaced by Conductor During Maintenance	Marginal	
	Open	N/A	Pumping/Standby	No Power Available to Power Relay 2 Contacts	High Thermal Environment; Excessive Current From Battery	High Output Current From Battery	Safe	
Power Relay 2	Coil Short	N/A	Pumping	A. Power Relay 2 Contacts Will Not Close; B. High Current Through Power Relay 1 Contacts Pressure Actuating Switch Contacts Timer Relay Coil	High Thermal Environment; Excessive Current From Battery	A. No Input on J04 Pin 2; B. High Voltage on J04 Pin 2 From Supply	Safe	Note: No Effect During Standby
	Coil Open	N/A	Pumping	Power Relay 2 Contacts Will Not Close and No Power Available at J03 Interface	High Thermal Environment; High Mechanical Shock; Excessive Current From J04 Pin 2	No Input on J04 Pin 2	Safe	Note: No Effect During Standby
	Contacts Closed	N/A	Standby	Power Circuit Complete to Pump Motor for Driving Pump	High Thermal Environment; High Mechanical Shock; Excessive Current From Fuse	Power Relay 2 Coil Energized From Power at J04 Pin 2	Marginal	
	Contacts Closed	N/A	Pumping	Pump Motor Circuit Complete After Normal Cycle	High Thermal Environment; High Mechanical Shock; Excessive Current From Fuse	Power Relay 2 Coil Energized From Power at J04 Pin 2 After Normal Cycle	Marginal	
	Contacts Open	N/A	Pumping/Standby	No Power Circuit Available to Pump Motor	Higher Thermal Environment; High Mechanical Shock	No Input to Power Relay 2 Coil on J04 Pin 2	Safe	If Pumping, the Contacts are Closed

Figure 5-7. Fault Hazard Analysis—Pumping Assembly

agencies responsible for specific types of equipment can often be informative; par. 5-3.6 identified these reports. Interviews with maintenance personnel and user organizations can provide insights into unsafe designs—insights that are not included in reliability data. Par. 2-3 lists additional sources of information.

5-4.4 ADVANTAGES

The advantages of conducting an FHA are

1. The FHA takes advantage of reliability program data to assist in developing the safety analysis.

2. Only those listings from an FMEA or FMECA that have safety connotations are carried over to the FHA as faults; this shortens and simplifies the FHA.

3. The FHA also contains information on subsystem faults that is not included in the FMEA or FMECA. These data include hazardous characteristics of subsystems, personnel errors, and environmental effects on safety.

4. The FHA includes information on upstream causes of faults that is not contained in an FMEA or FMECA.

5-4.5 LIMITATIONS

The chief limitation of the FHA is that in the case of failure faults resulting from multiple causes, the safety analyst cannot always trace all of those causes. Yet, the analyst, in examining faults—usually at the part or component level of the subsystem—is attempting to trace the fault to a hazardous condition or determine that a nonhazardous condition will exist as a result of the fault. The only multiple causes that the FHA can take into account other than errors are those involving the environment or common factors that might affect the fault being considered. To deal with equipment-related multiple causes, it is necessary to employ other techniques such as the fault tree analysis (FTA), discussed in par. 5-5.

5-5 FAULT TREE ANALYSIS
5-5.1 DESCRIPTION AND PURPOSE

A fault tree analysis (FTA) can be defined as the functional development of a specified, undesired event through logic statements of the causative condition. Thus an FTA is a detailed, top-down technique—a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event—that enables the analyst to search for the upstream cause of an identified fault to its ultimate source or sources. The FTA technique was developed by the Bell Telephone Laboratories, circa 1960, to present quantitative probabilities that specific undesired events could occur under a given set of circumstances. The specific undesired event in the initial study by Bell was the inad-

vertent generation of a trigger signal in an extremely complex military control system (Ref. 12).

A fault tree is not a model of all possible subsystem and system failure modes or possible causes of failure. The fault tree is tailored at its top event that corresponds to some particular mode. Thus the fault tree includes only those faults that can contribute to this top event. Moreover, these faults are not exhaustive, i.e., they cover only the credible faults as assessed by the analyst (Ref. 13).

Also, a fault tree is not in itself a quantitative model; it is essentially qualitative but can be evaluated quantitatively and often is used for this purpose. In a quantitative role the fault tree will indicate the specific reliability data required at all levels down to that of an individual part. The application of the reliability data can be used to determine the failure probabilities and risk assessment.

The FTA technique was developed because the inadequacies of some predecessor techniques limited their usefulness in safety analysis. For example, FMEAs and FMECAs could be used for qualitative and quantitative analyses but only when causes and effects of individual, independent hardware failures were considered. The PHA included potential failures, hazardous characteristics, personnel errors, and adverse environmental conditions; however, it lacked the means of arriving at probability predictions. Also the FHA and PHA could not always cope with the combined events leading to a failure. The FTA overcomes most of these limitations and treats fault events that can be associated with component hardware failures, human errors, and any other pertinent events leading to the undesired event.

In summary, the attractiveness of the FTA lies in the numerous benefits that can be derived from its use. It is a logical and systematic method that stimulates the insight of the system analyst toward deeper and deeper consideration of safety causes and effects. During the course of constructing the fault tree, much information will be learned about the system. In fact, this scheme of knowledge organization is useful precisely because it requires that the analyst know or make explicit assumptions about the relationships of the components that comprise the subsystem. The FTA is also an efficient method because it limits itself to only those factors related to a specific end result of interactive events and conditions. Thus, where the FMEA requires the consideration of failures for all components in a unit and the numerous possible effects of each failure, the FTA considers only those failures that would result in a single end effect. The existence of potential sources of "single-point failures"—an important consideration—can be identified from the logic diagrams that form the trees or from the mathematical expressions derived from the trees.

The relationships between the interconnecting branches of the fault can be conveniently reduced to precise

mathematical expressions. The mathematics of the FTA is presented in par. 5-5.1.1.

5-5.1.1 Use of Logic

One of the fundamental assumptions in FTA is that any of the events or conditions can exist in only one of two states at a specific time. These two states make up the entirety of possibilities. Thus the event or condition can be either on-off, open-closed, yes-no, true-false, high-low, etc. This limitation regarding bistable conditions is not as restrictive as it may appear. If a situation involves a condition that is neither entirely "open" or "closed", the analyst can list it as "partially open". The related bistable condition would then be "not partially open". Because of the existence of two states, a fault tree can always be translated into an equivalent set of Boolean equations.

5-5.1.2 Fault Tree Symbols

Two kinds of symbols are conventionally used in a fault tree—logic symbols, as shown in Fig. 5-8, and event symbols, as shown in Fig. 5-9. Each class of symbols is described in the paragraphs that follow.

5-5.1.2.1 Logic Symbols

Logic symbols are used to interconnect the events that contribute to the specified main top event. The basic symbols are the AND and OR Boolean logic gates symbolized by a shield with a flat or curved base, respectively. A discussion of each gate follows:

1. *AND Gate*. This gate is used to show that the output fault occurs only if all the input faults occur. A representation of an AND gate in fault trees is shown in Fig. 5-8(A). In order for the output Event D to occur, Events A_1, A_2, A_3, and A_4 must all occur. The Boolean algebraic expression for this AND gate is

$$D = A_1 \cdot A_2 \cdot A_3 \cdot A_4.$$

The AND gate also is referred to as a "times"(multiplication) gate because of the Boolean algebra relationship.

2. *OR Gate*. This gate is used to show that the output event occurs if only one or more of the input events occur. A representation of an OR gate in fault trees is shown in Fig. 5-8(B). Any of the inputs—i.e., B_1 or B_2 or B_3 or B_4—will cause the main output Event E to occur. The Boolean algebraic expression for this OR gate is

$$E = B_1 + B_2 + B_3 + B_4.$$

The OR gate also is referred to as a "plus" gate because of the Boolean algebra relationship.

5-5.1.2.2 Event Symbols

The event symbols associated with the fault tree are defined as follows:

(A) AND Gate
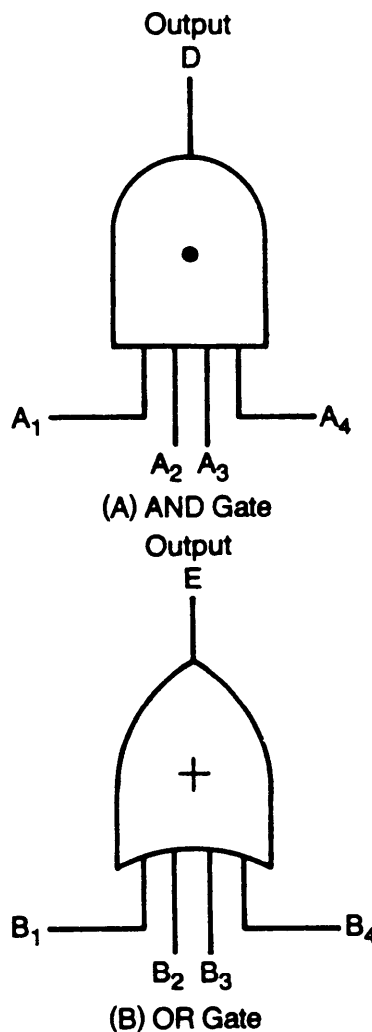
(B) OR Gate

Figure 5-8.   Logic Symbols

1. *Condition or Event*. A rectangle, Fig. 5-9(A), is used to represent a particular condition or event that is either the input or the output of an AND or an OR gate. If used for an input to a gate, it usually represents an existing condition that remains for the life of the item under investigation.

2. *Restriction or Conditional Situation*. An ellipse, Fig. 5-9(B), is used to identify restrictive or conditional situations that apply to a logic gate. When used with an AND gate, the restrictions or conditions must be fulfilled before the event above the AND gate can occur. When used with an OR gate, the ellipse may be used to indicate that the event above the OR gate cannot occur if all the inputs to the gate occur simultaneously.

3. *Basic Fault Event*. The circle, Fig. 5-9(C), describes a basic fault event that requires no further explanation. This symbol is used as an input to a logic gate.

4. *Event Normally Expected to Occur*. The house, Fig. 5-9(D), represents a situation or event that normally is expected to occur if no fault or malfunction occurs.

Output

Input

(A) Condition or Event

(B) Restriction or Conditional
Situation

(C) Basic Fault Event

(D) Event Normally Expected
to Occur

(E) Undeveloped Event

(F) Transfer (Output)

(G) Transfer (Input)
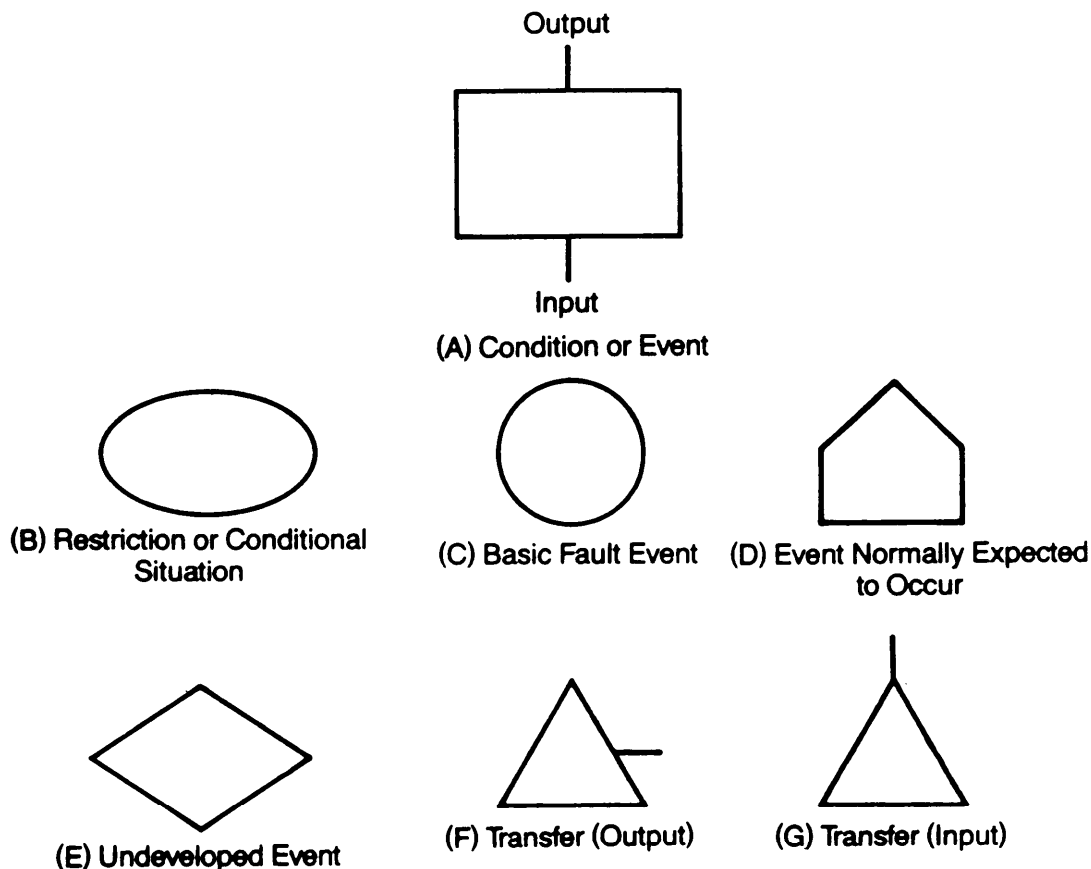
Figure 5-9. Event Symbols

5. *Undeveloped Event.* The diamond, Fig. 5-9(E), represents an event during which the analysis stops. The analysis may have stopped at this point because there is insufficient information to develop the situation further or because the results of further development are considered inconsequential.

6. *Transfer.* The triangles, Figs. 5-9(F) and (G), are used to transfer out of—a line from the side—or into—a line out of the top—other parts of the fault tree. A given situation in one part of the fault tree may cause something to happen in another part of the tree. Therefore, an output transfer symbol would be employed to show that information must be used at another point in the tree. The transfer input symbol would be used at the other point in the tree where the information is used.

5-5.1.2.3 Example of Use of Symbols

Fig. 5-10 is an example of a simple fault tree that illustrates the use of some of the symbols from Figs. 5-8 and 5-9. For a fire to start, three items usually are required: fuel (B), oxidizer (C), and an ignition source

(D)*. If one of these items is missing, a fire will not occur. Therefore, the diagram indicates that an AND condition exists.

The ellipse Z indicates a condition that must be satisfied before a fire will start, namely, the mixture of fuel and oxidizer must be within ignitable range when the ignition source is applied. If the ignitable mixture occurs *after* the ignition source has ceased, there will be no fire. In effect, the statement in the ellipse is another AND condition.

There can be several types of ignition sources, each of which could independently provide a satisfactory input to the AND gate. All of these possible sources—E, F, and G—therefore, are connected by an OR gate. Similar OR gates could be applied to Blocks B and C that indicate fuel and oxidizer if there were multiple sources of fuel and multiple sources of oxidizer.

If a fault tree is to be used only for qualitative purposes, the blocks and ellipses may simply be labeled to indicate

---

*It is assumed that the combination of B and C does not result in a hypergolic mixture and that B is not pyrophoric.
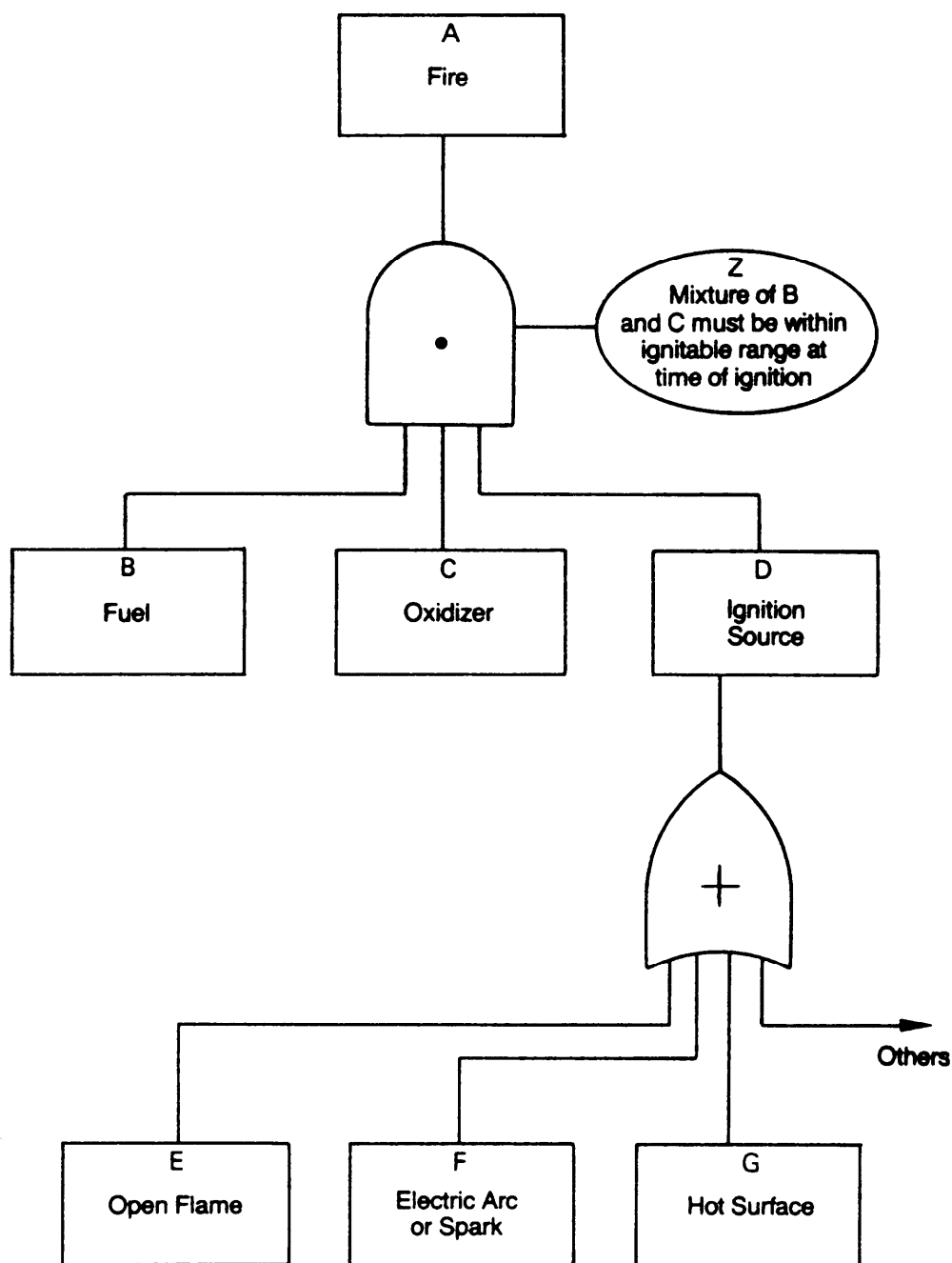
Figure 5-10.   Example of Simple Fault Tree Showing AND and OR Gates

the conditions or event under consideration, such as "Fire". When the tree is to be used for quantitative purposes, it is necessary to label the blocks and ellipses with terms that permit probabilities to be applied, such as "Fire Starts".

5-5.1.3   Events to be Analyzed

The top event identifies the potential problem whose possibilities of occurrence are to be determined, i.e., the top event must be established. For a given subsystem, there may be many top events; accordingly, the selection must be made with care and the initial fault tree configuration must represent the subsystem in its unfailed state. System boundary conditions (see par. 5-2.2) depend on which top event is selected. The initial conditions then become subsystem boundary conditions that define the component configurations for which the top event is applicable.

A safety analysis of a subsystem may involve many fault trees, each chosen for the study of one end result. Top events can be selected from numerous sources, some of which are

1. Problems known from past experience
2. Information from the PHA or other analyses
3. Requirements stated in specifications, standards, statements of work, or other documents.

Table 5-1 illustrates how top events could be chosen. The information in the table was excerpted from US Army Test and Evaluation Command (TECOM) Test Operating Procedure (TOP) 3-2-504 (Ref. 14). In Table 5-1 the first column gives the test requirement as stipulated in Ref. 14. These test requirements are, in reality, a statement of the condition of the weapon to be tested. The second column provides the pass/fail criterion for each test; also it shows how a suitable design-specification requirement might be written. The third column shows the top event for a fault tree that could be used to show how the weapon could fail that particular test requirement.

Since the information in Column 1 of Table 5-1 represents requirements for tests to be conducted on a weapon, it may appear that an FTA is not necessary; however, this is not the case. The tests may not reveal design deficiencies that are low probability events, but a thorough FTA may identify faults that are not discovered by test. Tests will verify, to a degree, the adequacies of the analyses. Therefore, both tests and analyses should be conducted.

5-5.1.4 Tree Development

After the top event is selected, the analyst begins developing the tree by identifying all events and conditions that can contribute to the top event. Each such event or condition is categorized as a

1. *Primary Failure*. Failure of a component or device that occurs while it is operating with normal inputs and within design limits
2. *Secondary Failure*. Failure of a component or device caused by an abnormal environment, input, or other condition outside of design limits—e.g., excessively high temperature, vibration, or impact
3. *Commanded State*. Component or device state or event due to an abnormal, erroneous, or untimely input— e.g., a timing error or a power input due to a short circuit. Note that these three categories do not include hazardous characteristics. If a component or assembly has a hazardous characteristic(s) that could have an effect on the failure identified in the top events, this hazardous characteristic(s) must be included in the fault tree.

Here it is important to distinguish between a fault and a failure. If a switch, for example, failed to close when a voltage was impressed across its terminals, this would be a failure of the switch. However, if the switch closed at the wrong time due to the improper functioning of an upstream event, this would be a system failure, not a switch failure. This illustrates that all failures are the results of faults, but not all faults produce failures.

TABLE 5-1. SELECTING TOP EVENT FOR FAULT TREE (Ref. 14)

TOP Par. Number	TOP 3-2-504 Test Requirement Statement	Design Specification	Fault Tree Top Event
5.3.1a	(1) Place the safety selector in the SAFE position with the test item cocked, and conduct a minimum of 10 dry firing attempts to intentionally override the safety.	Weapon shall not fire with safety selector in SAFE position when weapon is cocked.	Weapon fires with safety selector in SAFE position.
	(2) Place the safety selector between SAFE and FIRE positions and repeat Step (1).	Weapon shall not fire with safety selector between SAFE and FIRE positions.	Weapon fires with safety selector between SAFE and FIRE positions.
5.5	Determine whether the weapon can be fired without the bolt or barrel (if quick change type) being completely or adequately locked.	Weapon shall not fire when bolt or barrel (quick change type) is not completely or adequately locked.	Weapon fires when bolt or barrel is not completely or adequately locked.
5.7	Determine whether it is possible to assemble the weapon incorrectly so that it can be fired in an unsafe condition.	Weapon shall be designed so it cannot be incorrectly assembled in a way which will permit it to be fired in an unsafe condition.	Weapon fires in unsafe condition because of incorrect assembly.

The fault tree is extended down through its branches. Each event in a path is examined to determine the factors that could cause it. The tree ends when the branches reach the point at which all foreseeable input events are included—i.e., component failure, personnel error, hazardous characteristic, or environmental effect. The resultant tree will be such that reading down the tree will indicate all of the possible courses of events and reading up will give the effects of events.

The upper levels of a fault tree often can be prepared concurrently with a PHA, in which case the two analyses will be mutually beneficial because information from the PHA will identify hazards useful to the FTA, and the FTA, in turn, can assist in identifying some of the related data—causes of hazards—to feed into the PHA.

5-5.1.5 Evaluating the Tree

Any set of basic events or conditions whose occurrence causes the top event to occur is referred to as a "cut set". A minimal cut set is the smallest combination of basic events or conditions which, if they all occur, will cause the top event to occur. A fault tree should include *all* possible paths, or cut sets, that could lead to the top event. Frequently, it is desirable to determine whether the events and conditions in one cut set are more likely to produce the top event than are those in other cut sets. The priority for corrective action should be for the more likely cut sets.

From the events, conditions, and their interrelationships in a tree, an analyst may be able to recognize whether the possibility of a single-point failure exists, i.e., a failure in which an accident could result from one component loss, human error, or other single untimely event. Fig. 5-11 contains six diagrammatic expressions of single-point failures. Some of these single-point failures, such as the ones in Figs. 5-11(A) and (B), are obvious; others are not obvious. An explanation of some diagrams in Fig. 5-11 follows:

1. *Conditional Straight Line (Operating)* (Fig. 5-11(C)). There is an AND gate leading into the top event, M, indicating that both E and F must occur for M to occur. However, the symbol for E, the "house", shows that E will always be present when the system is operating unless a failure occurs. Therefore, under normal conditions, only F must occur to cause M to occur. Thus Event F can cause a single-point failure.

2. *Uninhibited Paths* (Fig. 5-11(D)). The top event, A, can be generated by the occurrence of either X, or Y, or Z since there is no inhibiting AND gate between Events X, Y, and Z and the top event.

3. *Redundant Failures* (Fig. 5-11 (E)). Because of the AND gate just before Event P, it is necessary for both Events S and T to occur in order for Event P to occur. Note that each path has an Event G in it. If Event G occurs, then Events S and T will occur and Event P will occur since OR gates lead to Events S and T. Since Event

G is in both paths, it is called a redundant failure. The analyst should be alert for this type of event when transfer symbols indicate that events occur in more than one path.

4. *Redundant Failures Involving a Subset* (Fig. 5-11(F)). The situation necessary for Event R to occur is similar to that for Event P (Fig. 5-11(E)), only in this case, G′ is a subset of G. If Event G occurs, Event G′ will occur also since G′ is a subset of G. The reverse of this is not true, however, i.e., the occurrence of Event G′ will not cause Event G to occur. Sometimes it is not readily apparent that one event or condition is a subset of another. Nevertheless, such determination of interrelationships is necessary not only to discover single-point failures but also to eliminate redundancies that may affect quantitative analysis.

It is very desirable to eliminate single-point failures, but in some cases it is impossible or economically unjustifiable to do so. The possibility of occurrence of a single-point failure can be accepted if

1. The probability of occurrence of the undesired event it initiates is so low that the undesired event is improbable (Level E, par. 5-3.4.3).

2. The consequences of such an occurrence are inherently insignificant.

3. Actions are taken to contain any significant effects.

A fault tree will be required for these three situations only if it is necessary to identify the single-point failure that initiates the top undesired event and/or to determine the probability of occurrence.

5-5.1.6 Simplifying the Tree

Completed fault trees may contain redundancies that, unless removed, will distort the probability of occurrence of a top event. The redundancy may consist of

1. The same events or conditions in parallel branches

2. Events or conditions in parallel branches that are subsets of other events or conditions.

The fault trees can be simplified by expressing in Boolean algebra the AND/OR relationships in the tree. The initial Boolean algebraic equation is simplified by expansion, combination, or elimination of terms. The resulting equation is used to construct the simplified fault tree. If probabilities of occurrence of events have been assigned, they can be inserted into the resultant Boolean equation to calculate the probability of the occurrence of the top event.

A fault tree with a redundant event is shown in Fig. 5-12(A) (Ref. 11). By use of Boolean algebra, the top event can be expressed as

$$K = X \cdot Y = (B + C)(B + D) \qquad (5-5)$$

where

(A) Straight Line

(B) Multiple Straight Line

(C) Conditional Straight Line (Operating)

(D) Uninhibited Paths

(E) Redundant Failures

(F) Redundant Failures Involving Subset
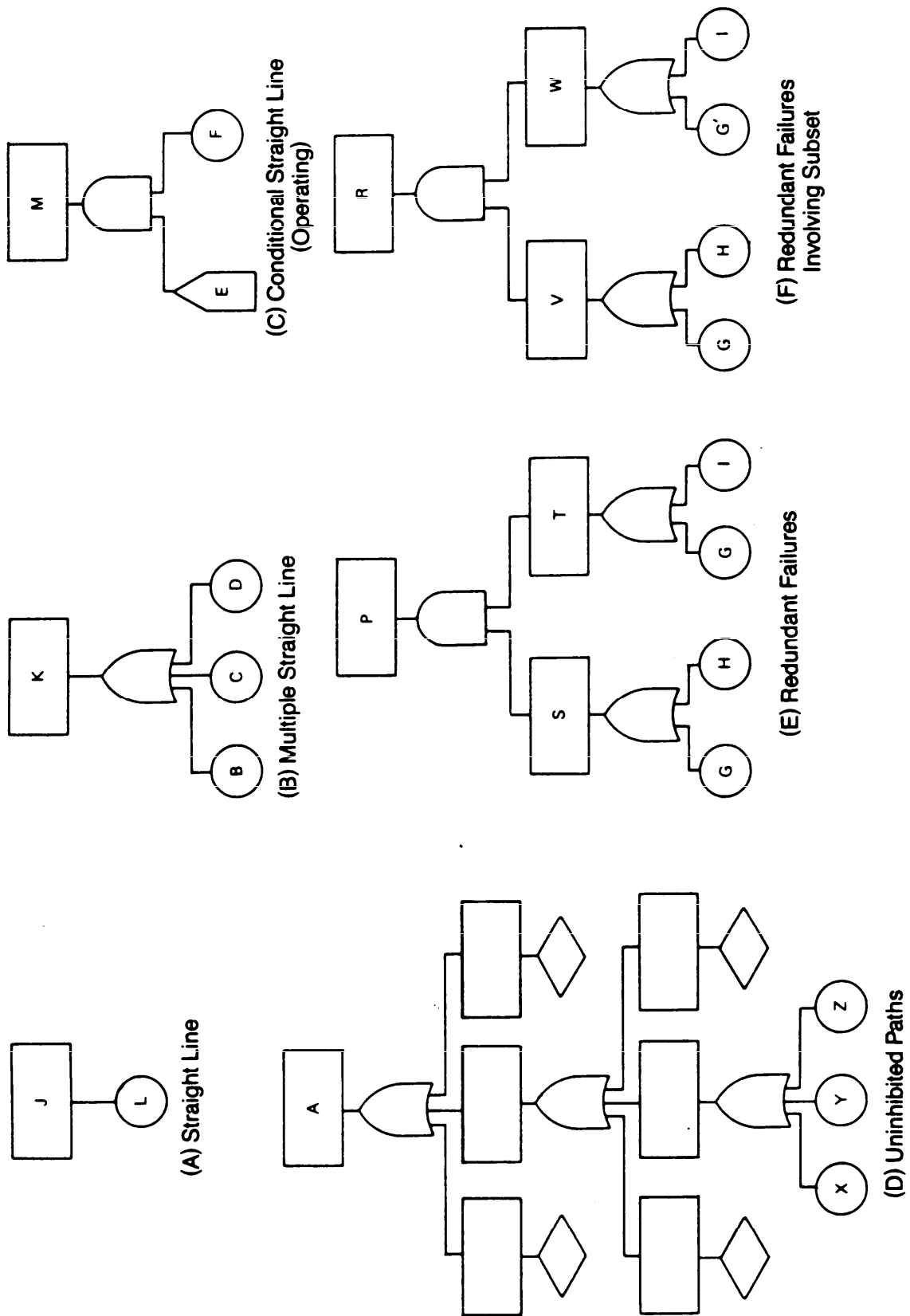
Figure 5-11.   Single-Point Failure Indicators in a Fault Tree
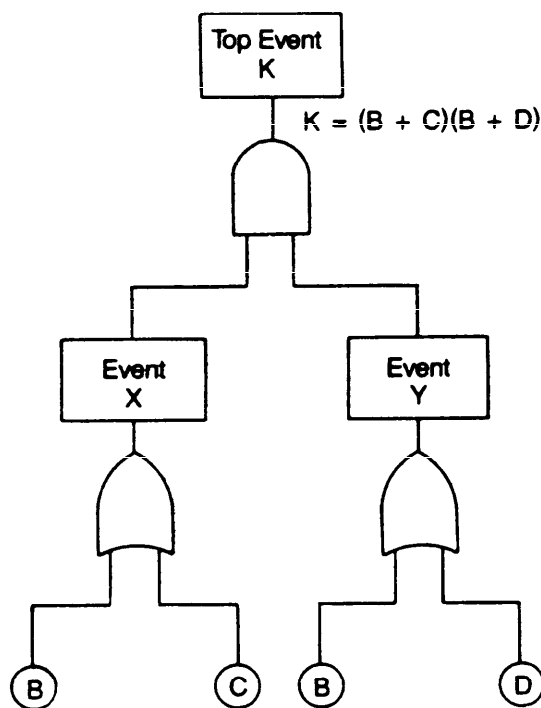
(A) Original Tree   (B) Simplified Tree
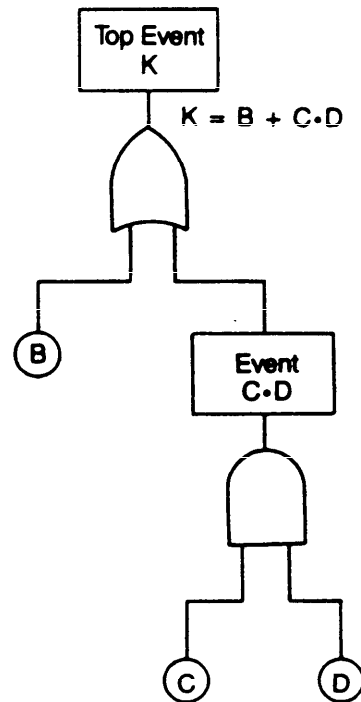
Figure 5-12.   Simplification of Fault Tree (Adapted from Ref. 11)

( )( ) and · = AND relationship*
  + = OR relationship*.

According to the rules of Boolean algebra, Eq. 5-5 can be expanded by the distributive law to

$$K = B \cdot B + B \cdot D + B \cdot C + C \cdot D. \quad (5\text{-}6)$$

By applying other rules of Boolean algebra, $B \cdot B = B$ by the idempotent law, and $B \cdot D$ and $B \cdot C$ are included in B. The fact that $B \cdot D$ and $B \cdot C$ are included in B is evident from a Venn diagram, i.e.,

where the shaded area obviously is included in B.

$B \cdot D = B \cap D$
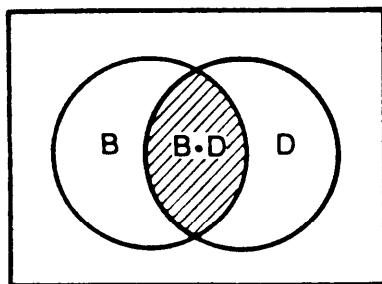
where the shaded area obviously is included in B.

$B \cdot C = B \cap C$
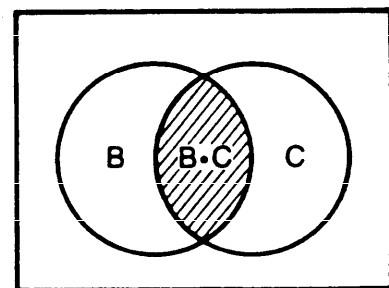
From Eq. 5-6

$$K = (B + B + B) + C \cdot D \quad (5\text{-}7)$$

which reduces by the idempotent law to

$$K = B + C \cdot D. \quad (5\text{-}8)$$

By using Eq. 5-8, the fault tree can be redrawn as shown in Fig. 5-8(B).

If Events B, C, and D are assigned failure probabilities as follows

$B = 1.5 \times 10^{-3}$ failures per selected period
$C = 4.0 \times 10^{-4}$ failures per selected period
$D = 2.0 \times 10^{-4}$ failures per selected period,

*The AND relationship is also referred to as the "intersection" (symbol ∩) of events attached to gate. The OR relationship is also referred to as the "union" (symbol ∪) of events attached to gate.

(A) Original Tree   (B) Simplified Tree
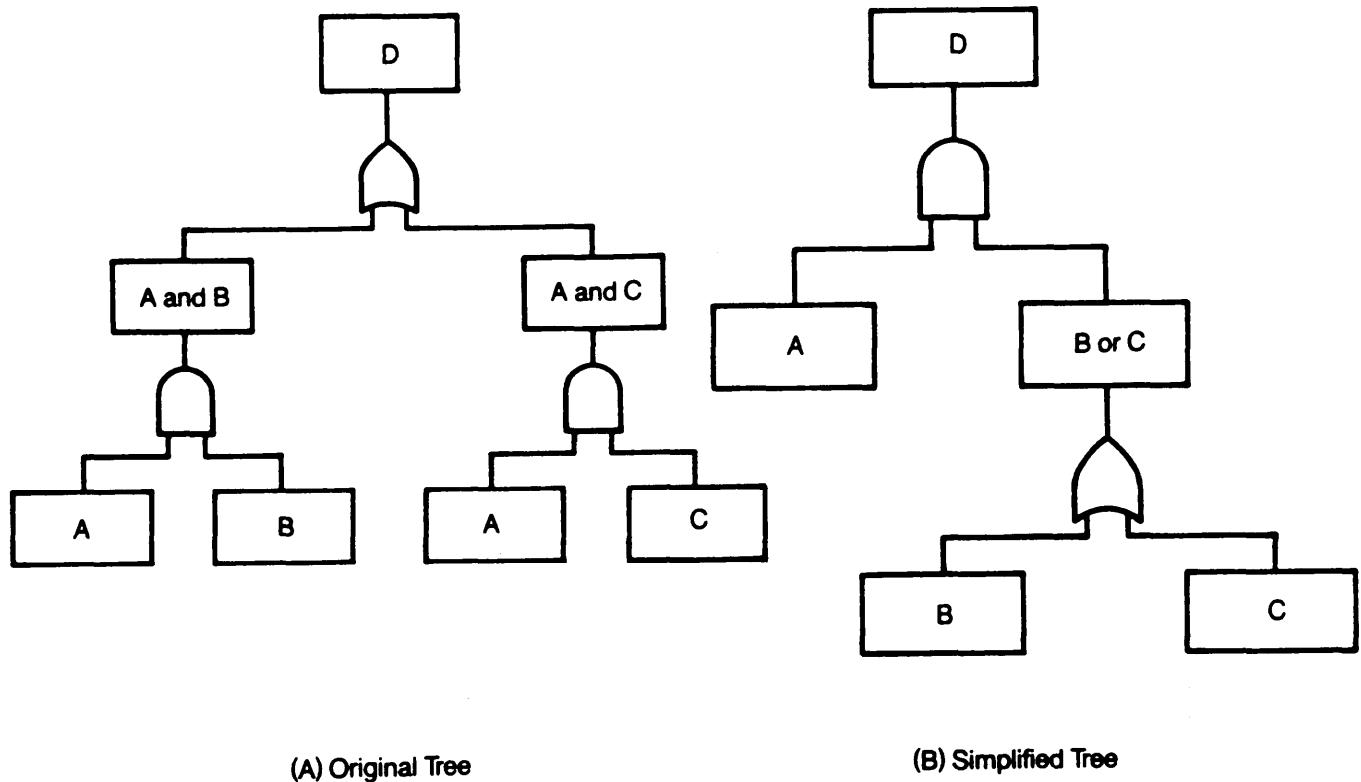
Figure 5-13.   Equivalent Fault Trees

the probability of the occurrence of Event K can be calculated. If Eq. 5-8 is used, the probability of Event K is

$$K = 1.5 \times 10^{-3} + [(4.0 \times 10^{-4})(2.0 \times 10^{-4})]$$
$$= 1.50008 \times 10^{-3}.$$

If the original tree had not been simplified and Eq. 5-5 reduced, the calculated *incorrect* value of K would have been

$$K = (1.5 \times 10^{-3} + 4 \times 10^{-4})(1.5 \times 10^{-3} + 2 \times 10^{-4})$$
$$= 3.23 \times 10^{-6}. \text{ (An error of three orders of magnitude.)}$$

Thus this example illustrates the need to simplify fault trees to eliminate redundancies.

In some cases fault trees with redundancies can be simplified to remove the redundancies, but the probability of occurrence of the top event will not change. As an example, consider the fault tree in Fig. 5-13(A). The Boolean algebraic equation for Event D in Fig. 5-13(A) is

$$D = (A \cdot B) + (A \cdot C) \qquad (5-9)$$

By the distributive law of Boolean algebra, Eq. 5-9 can be reduced to

$$D = A \cdot (B + C). \qquad (5-10)$$

By using Eq. 5-10, the fault tree can be redrawn as shown in Fig. 5-13(B). If Events A, B, and C are assigned failure probabilities as follows

$A = 2 \times 10^{-3}$ failures per selected period
$B = 2 \times 10^{-4}$ failures per selected period
$C = 3 \times 10^{-4}$ failures per selected period,

the probability of occurrence of Event D can be calculated. If Eq. 5-9 is used, the probability of Event D is

$$D = [(2 \times 10^{-3})(2 \times 10^{-4})] + [(2 \times 10^{-3})(3 \times 10^{-4})]$$
$$D = 4 \times 10^{-7} + 6 \times 10^{-7}$$
$$D = 10^{-6} \text{ failures per selected time.}$$

The probability of Event D from Eq. 5-10 is

$$D = 2 \times 10^{-3}(2 \times 10^{-4} + 3 \times 10^{-4})$$
$$D = (2 \times 10^{-3})(5 \times 10^{-4})$$
$$D = 10^{-6} \text{ failures per selected time.}$$

As can be seen from this example, the fault tree can be simplified to remove the redundancy, but the probability

of occurrence of the top event remains the same. The reason the probability of D remained the same is that Eqs. 5-9 and 5-10 are equal from a purely algebraic point of view. Eqs. 5-5 and 5-8 are equal from a Boolean algebraic point of view; however, they are not equal from a purely algebraic point of view. Consequently, Eq. 5-8 gave the correct probability of the top event.

The rules for simplifying a fault tree with a redundancy follow:

1. Write the Boolean algebraic equation for the top event.

2. Use the rules of Boolean algebra to simplify the equation for the top event to the maximum extent possible.

3. Draw a new fault tree to satisfy the simplified equation for the top event.

4. If the probability of the occurrence of the top event is needed, use the simplified equation for the top event to calculate the probability.

Another value of the simplified fault tree is that it is easier to recognize events or conditions that could cause single-point failures. Note from Fig. 5-12(B) that Condition B is a single-point failure.

5-5.1.7 Other Uses of Fault Trees

The logical approach inherent in the fault tree methodology has led to a variety of other uses. Some of these uses are

1. The use of fault trees permits the elimination of redundancies that otherwise might result in an incorrect equipment failure rate calculated from the failure rate of the individual components.

2. When the top event selected for a fault tree is that the subsystem will not operate satisfactorily, the resulting fault tree will indicate all the events and conditions that would lead to unsatisfactory operation. This analysis of the fault tree could indicate potential troubleshooting problems that may occur during maintenance of the subsystem.

3. Fault trees may be used for accident investigations. The top event is the immediately apparent accident. The tree consists of all events and conditions that could cause or contribute to that accident. An investigator would eliminate the events or conditions that evidence showed did not or could not occur. The remaining items in the fault tree will point to the cause or causes of the accident.

4. By using probabilities of occurrence of accidents and of potential dollar losses, risk assessments may be made to determine whether specific corrective actions, preventive measures, or changes in design are economically justifiable.

5-5.2 ANALYSIS TECHNIQUE AND FORMAT

5-5.2.1 Technique

One of the principal merits of a fault tree analysis is the progression that occurs during its accomplishment. The tree evolves as the consideration of each event or condition brings to mind more and more events or conditions that can cause or contribute to the top event. A logical progression of steps is followed in conducting an FTA, i.e.,

1. Select the top event.

2. Identify the subsidiary events and conditions that, alone or in combination, can cause the top event.

3. Determine whether or not each of these events or conditions by itself can cause that top event or whether all events or conditions are required simultaneously or in various combinations. This information is then diagrammed with suitable logic symbols and stipulations.

4. Identify the events and conditions that can cause each subsidiary event or condition. Repeat the process until the tree reaches basic information such as component failures, errors, hazard characteristics, or an adverse environmental condition.

5. If desired, the analyst can conduct or have conducted a failure mode analysis of each component failure shown on the tree.

6. Examine the tree and each cut set to determine whether there is any arrangement that could lead to a single-point failure.

7. Determine how each basic event at the bottom of the tree can be minimized. The responsible organization should then be notified regarding the need to take action to minimize the possibility of occurrence of that event or condition.

8. If a quantitative analysis is to be accomplished and if the tree is small, develop the Boolean equation and simplify it. If the tree is large, the use of a computer may be necessary to perform the quantitative analysis. Ref. 15 provides information on the computer-aided synthesis of fault trees.

9. Enter available, required reliability and other probability data into the Boolean equation. Where data are not immediately available, they can be obtained by Monte Carlo or other simulation techniques.

10. Determine the probability of occurrence of the top event. Where desired, the probabilities of the top event along each cut set can be calculated to determine the most critical path (the path with the highest probability of occurrence).

5-5.2.2 Format

The basic format of a fault tree has already been presented through the diagrams in Figs. 5-8, 5-10, and 5-11.

Fig. 5-9 gives other symbols that may be used in a diagram if needed. The condition or fault could be written within the symbol, as shown in Fig. 5-14. This approach is satisfactory provided the fault, condition, or event can be described in a few words. Another possible approach to identifying the parts of the diagram is to number the parts on the diagram, as shown in Fig. 5-15. A table can be constructed indicating the numbers and the condition or fault related to that event. Other columns could be added to the table to provide additional information as desired. Since the numbers grow larger (more digits) as the number of levels increases, this approach is limited to reasonably small trees. For large trees the assistance of a computer will be required. Regardless of the approach adopted, however, a bookkeeping system must be established to keep track of each item, its status or conditions to be considered, and its position in the hierarchy. Unless a strict discipline of labeling of items and their status is followed, errors in identifying items may occur—e.g., two different codes may be assigned to the same item.

5-5.3 SOURCES OF DATA

Top events can be selected from such sources as past experience and general knowledge of problems that potentially existed or occurred with predecessor systems; specifications, standards, and similar documents; and deliberative considerations of potential accidents. Results of accident investigations obtained from organizations listed in par. 4A-1, Appendix 4A, are also helpful in indicating potential adverse events that should be investigated. Par. 2-3 provides additional sources of information.

Information on the workings of subsystems subjected to FTA is best obtainable from the designers because they can describe how the subsystem will operate, the assumptions and data on which the design was based, potential malfunctions that they have foreseen, and methods they have employed to control the occurrence of adverse effects.

Data on component failures can be obtained from sources listed in par. 4A-2, Appendix 4A, documents in the bibliography of this chapter; and FMECAs made prior to the FTA. Reliability information, especially for electronic components, can be obtained from Ref. 8 or manufacturers. One note of caution concerning data from manufacturers: Manufacturers often are overly optimistic about their products.

5-5.4 EXAMPLE

The example presented is taken in part from Larsen's analysis of the safing and arming (S&A) device, XM813, of the SHILLELAGH missile (Ref. 16). The part of the analysis shown here relates only to the qualitative portion. The Boolean algebraic expression for the top event

investigated and the derivation of the probability of occurrence are included in Ref. 16.

Before proceeding with the analysis, it should be noted that the safety design goal for Army materiel is to eliminate single-point failures that could result in an undesired event. This goal is not achieved, however, in every case because the cost or requirements necessary to remove the single-point failure of a severity Category IV with Frequency E may or may not warrant the removal. In the case of an undesired event of severity Category I, regardless of frequency, however, the single-point failure must be removed—e.g., in a system containing high explosives that could be initiated by the single-point failure. In the case of the S&A device, XM813, when a single-point failure was identified, an inhibiting design feature—such as a rotor assembly—was added to the S&A system to prevent a single-point failure to cause the top unwanted event to occur. A great deal of information can be obtained about the electromechanical S&A device, XM813, by subjecting it to an FTA.

Fig. 5-16 shows the basic information about the S&A device, XM813, for developing a fault tree to investigate the possibility that the fuze might arm and the detonator might fire prematurely while the SHILLELAGH missile is still in the gun tube. The fault tree for the XM813 device is shown in Fig. 5-14. The symbol Y_2 on the fault tree No. 2 AND gate transfers information from the S&A tree in Fig. 5-14 to another fault tree (not shown here) and also to condition Gate No. 11. The S&A device and its functioning are described in the next paragraph.

The S&A device is a hermetically sealed unit that contains a mechanical acceleration-sensing mechanism. As shown in Fig. 5-16, the explosive train consists of an electrically initiated detonator in an unbalanced rotor and a lead fixed in the base of the housing. The rotor has a cantilever switch that shorts the detonator in the unarmed position (Fig. 5-16(A)) but completes the electrical circuit to the detonator when in the armed position (Fig. 5-16(B)). A clock mechanism controls the rotation of the rotor. A brass bias weight unlocks the rotor when the missile accelerates and allows the rotor to rotate into the armed position. At rest, the bias weight is restrained by two helical compression springs mounted on the bias weight guideposts. The bias weight has a decal with the letters "S" (for safe) and "A" (for armed), which can be viewed through a port in the housing to determine visually whether the unit is in the armed or safe position. Electrical power is supplied by an on-board missile battery. When the launched missile impacts, the double ogive (contact switch) in the warhead makes contact, the electrical circuit is completed through the S&A rotor and wire harness, and the detonator is fired.

Fig. 5-14 shows the completed fault tree for the possibility that the fuze arms and the detonator fires prematurely in the gun tube. After an examination of the interrelationships of the events and conditions and consideration
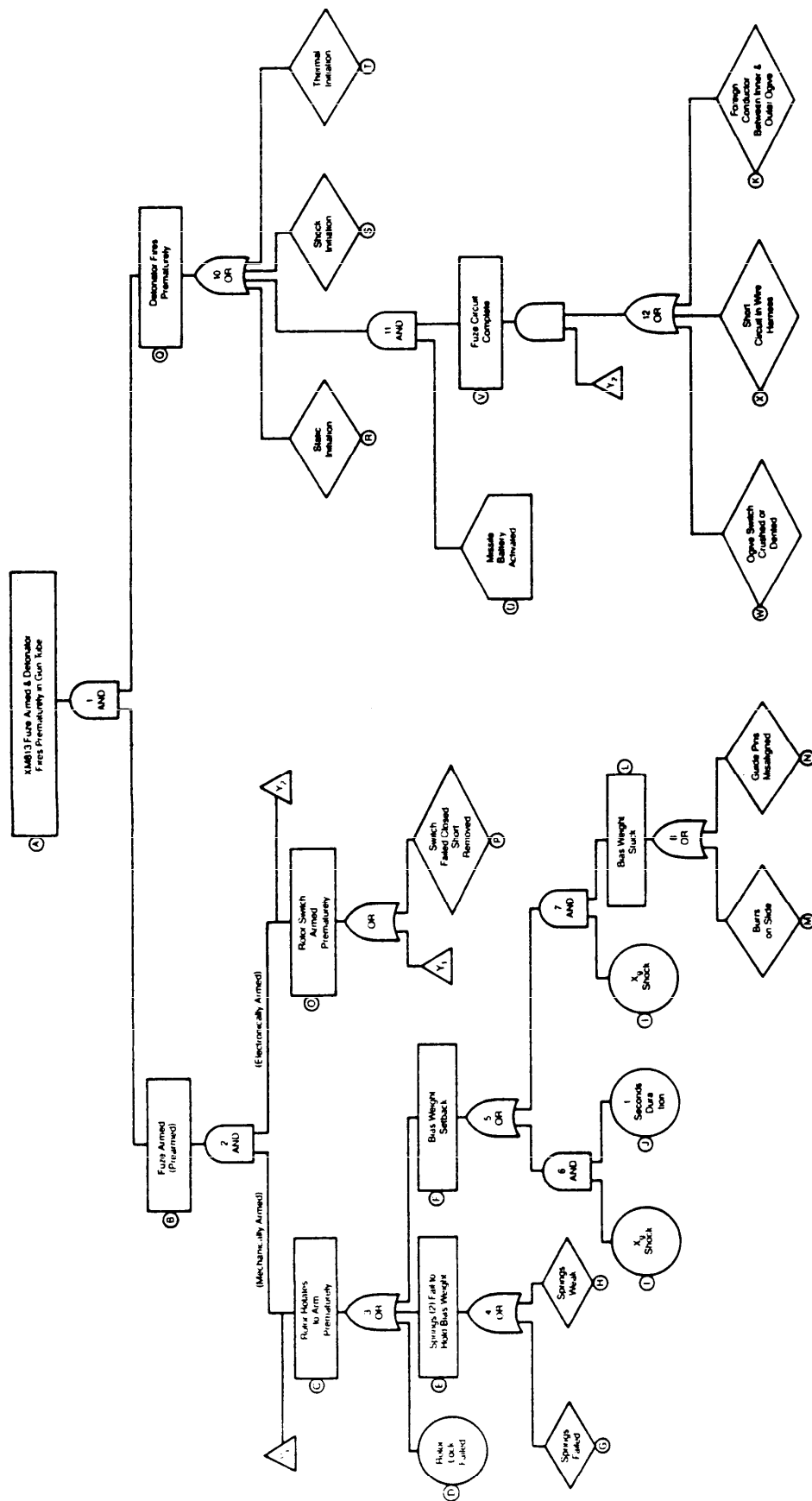
Figure 5-14. Fault Tree Analysis of XM813 S&A Device (Ref. 16)
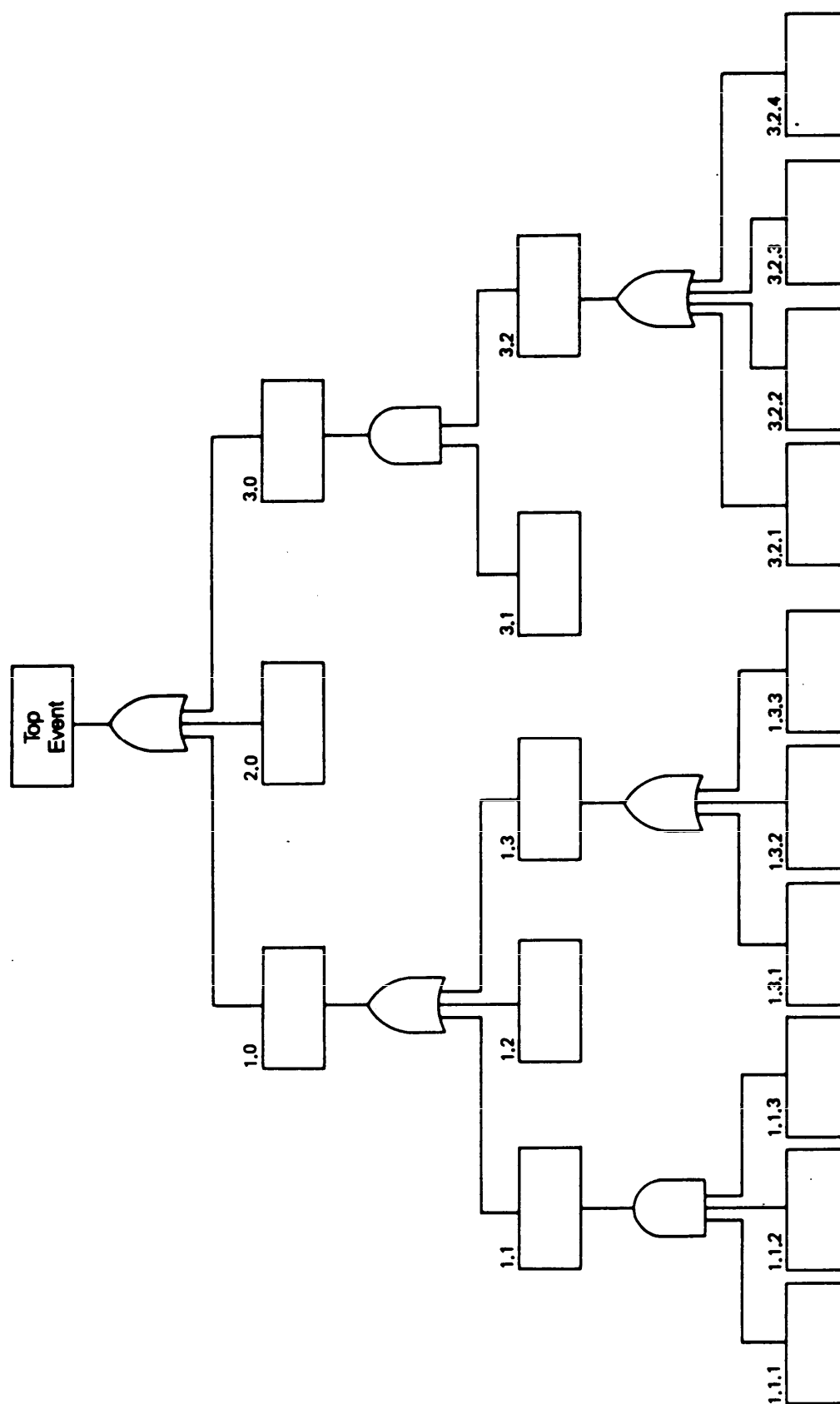
Figure 5-15. Numbering System Useful for Small Trees
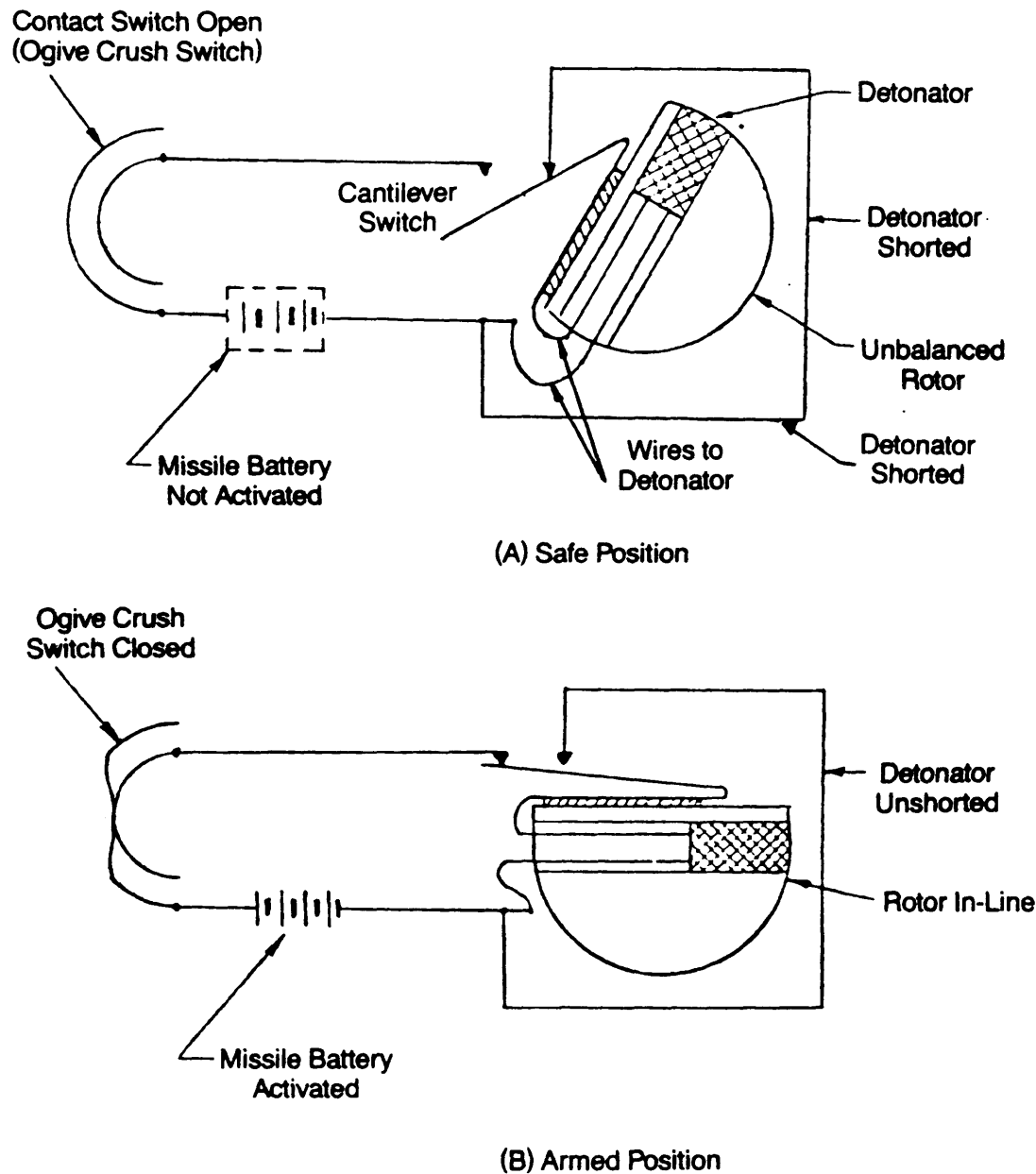
Figure 5-16.   XM813 S&A Device (Ref. 16)

of the fuze functional design and its mechanization (how the hardware implements the functional design), the following comments can be made:

1. If, for any reason, the fuze is mechanically armed (left-hand branch), any of the cut sets in the right-hand branch—which could cause the detonator to fire prematurely—would be single-point failure events or conditions. Those labeled, R, S, and T are readily apparent. The cut sets that provide inputs to AND Gate No. 11 are actually examples of the potential single-point failure condition shown under M in Fig. 5-11(C). In Fig. 5-14 the tree branch B normally inhibits these single-point failures

from firing the detonator. Once the missile battery is activated, each of the defects shown in W, X. or K (right-hand side of Fig. 5-14) would cause the detonator to fire prematurely (again, only if the fuze has been armed electrically at (O) (left-hand side of Fig. 5-14)).

2. The defects indicated in W, X, and K could have been generated only during the manufacturing process, handling, transporting, or maintenance of the round. This information should be used to alert personnel to the need for care during production, handling, transportation, and maintenance and to alert quality engineering personnel to the need for means to test the device to insure

that none of these defects exists before the device is incorporated into a higher level assembly. A visual inspection for dents in the nose area is required before using the round. A dent is cause for rejection because firing a round with a W, X, or K defect may cause the detonator to fire at the instant the fuze armed. Whether the detonator would initiate detonation of the warhead is a further function of the timing between the rotor switch making contact and the detonator being aligned with the powder lead. Normally, this would occur at what is considered a safe distance in front of the firing position, but troops in a forward position could be in the danger zone.

3. The analyst should review the circumstances whereby the missile battery is activated so that if W, X, or K does exist and the fuze is electrically armed, the conditions for firing the detonator and the consequences—whether the warhead can be detonated prematurely—can be identified. The analyst should also investigate to determine whether the rotor timing parameters will permit the detonator to fire prematurely, i.e., before the rotor is fully rotated mechanically. This condition probably would result in a dud round.

4. The condition FUZE ARMED (PREARMED) (fuze arms prematurely.) also appears to be dependent on the output of AND Gate No. 2. This AND condition is illusive since both inputs to the AND gate can be satisfied by the same acceleration and rotor rotation events, i.e., those under the transfer symbol Y_1. This type of arrangement, that can lead to a single-point failure, is shown under P in Fig. 5-11(E).

5-5.5 ADVANTAGES

The advantages resulting from an FTA follow:

1. Because the FTA proceeds from the adverse effect whose possibility of occurrence is to be analyzed—considering only information on events and conditions related to that event—nonpertinent information, events, and conditions are omitted. Since only the parts of a subsystem affecting the undesired event are analyzed, the FTA becomes an efficient tool for reducing cost, time, and paperwork associated with the analysis.

2. The FTA is an effective tool by which the safety engineer can burrow into an existing or proposed system design, isolate the most important troublemakers, and link and identify complex combinations of events and conditions which could result in an accident. By the use of Boolean algebra the analyst can reduce the complex to its simplest terms for further study. Without the benefit of an FTA, failure combinations leading to the cause of the undesired event may not have been uncovered.

3. If conducted early enough, an FTA can assist in the elimination of costly design changes and retrofits.

4. An FTA includes external influences, e.g., environmental factors and human interactions, which are not accommodated by an FMEA or an FMECA.

5. An FTA can become extremely detailed in presenting both the events and conditions which can occur and their interrelationships.

6. Because the FTA is a diagrammatic presentation, it is relatively easy to observe the causes, effects, and interrelationships of subsystem components. Each entry tends to alert the analyst to lower-level events and conditions which could contribute to the cause of that entry. Each entry alerts the analyst to consider additional factors that could affect the top event.

7. An FTA can be used beneficially for both a qualitative and quantitative analysis.

5-5.6 LIMITATIONS

Although FTA is being used increasingly by analysts, it does have limitations, i.e.,

1. A fault tree is a logic diagram that includes only causes and effects of conditions and events and their interrelationships. It, therefore, must be supplemented with additional material to make it informative to a reviewer.

2. Computerizing quantitative analyses of complex fault trees is extremely useful in terms of time and money savings over the cost of manual analysis. However, in fault trees that contain over 200 events or conditions, the simplifications of Boolean equations and computations of probabilities of occurrence of top events may require considerable computer time. This is especially true when occurrence of these events or conditions may be intermittent or subject to limiting conditions or when simulations such as Monte Carlo techniques must be used.

3. The selection of nomenclature for each event and condition in a tree to be used for a quantitative analysis must be such that a suitable probability can be applied. The adequacy of the nomenclature for the application of probabilities will depend on the skill of the analyst selecting them.

4. In the construction of the fault tree it may be difficult to distinguish between dependent and independent events.

5-6 SNEAK CIRCUIT ANALYSIS

Beginning in late 1967, the Boeing Aerospace Company and the Convair Division of General Dynamics developed a computer-aided electrical system analysis technique to help assure the trouble-free operation of the National Aeronautics and Space Administration's (NASA) APOLLO and SKYLAB hardware. This technique—some elements of which are proprietary to the Boeing Company—is referred to as "sneak circuit analysis" (SCA). The analysis has since been applied successfully to a variety of aerospace, military, and commercial projects with beneficial results. The technique has proven particularly beneficial for circuitry containing manual switches, relays, transistors, and digital logic. A review of a number

of unexpected occurrences suspected of resulting from sneak circuits highlighted these notable incidents (Ref. 17):

1. Missiles accidentally launched

2. Bombs accidentally armed and dropped

3. Aircraft electrical system "unannounced failures" that led to crashes

4. Electric utility lineman electrocuted

5. Hydraulic analog wherein fire alarms were initiated falsely at a public school by the automatic sprinkler monitoring system.

Accordingly, since sneak circuits apparently are universal in complex electrical and electronic systems and are a cause for concern with respect to safe, efficient, and reliable operation of a system, MIL-STD-785 (Ref. 5) provides for the conduct of an SCA. Since the conduct of an SCA is costly and time-consuming, it should be reserved for components and circuitry which are critical to mission success and safety (Ref. 5).

5-6.1 DESCRIPTION AND PURPOSE

A sneak circuit is defined as a designed-in signal or current path that causes an unwanted function to occur or which inhibits a wanted function (Ref. 18). SCA is a formalized, systematic approach used to determine whether electrical hardware contains latent (sneak) circuit paths that will result in unplanned modes of operation. It is emphasized that the sneak circuit conditions are latent in nature—present but not always active—and are not dependent on component failures, although many sneak-circuit-caused erroneous responses or system failures may have been attributed to component failures. Thus SCA is not the type of activity performed by engineers in the normal acquisition process of materiel. Programs that can benefit most from SCA—especially if begun in the preliminary design stage to allow early (paper) fixes to the discovered problems—are those involving multiple contractors, high change rates, or complex systems. It is further emphasized that an SCA is not an FMEA, FMECA, FHA, or FTA, neither is it a by-product of these analyses.

Experience in performing SCAs has shown the following to be the primary causes of sneak circuits:

1. *Changes*. Revisions to original designs may generate paths where sneak circuits can occur; complete integration, or consideration, or testing of all operational modes is not always a part of a modification process.

2. *Design Oversights*. A large and/or complex system can make a system overview extremely difficult. The far-reaching effects of each portion of a circuit must be known to assure that all functions performed as desired. The designer, production engineer, analyst, and other personnel responsible for a system may be unaware of or not recognize conditions that spawn problems in test or operation.

3. *Incompatible Design*. Designs prepared by different independent designers or design organizations may result in incompatibilities when the assemblies or other components are integrated into one subsystem.

4. *Fixes*. Malfunctions observed during testing are occasionally corrected by field "fixes" that solve the immediate problem but also generate other problems that are not recognized immediately.

5. *Human Errors*. Errors can contribute to the occurrence of sneak circuits in several ways. When operators are in a control loop, the possibilities for unanticipated modes of system operation increase—even with highly trained teams and detailed procedures. For example, manual operations may be performed out of sequence and procedures may not always be followed, and these situations may allow sneak circuits to result which otherwise would not be encountered.

The previous statements explain the possible causes of sneak circuits in materiel. The following are descriptions of the four basic categories of sneak circuits that these cause actions result in

1. *Sneak Paths*. Latent paths in designed circuitry, even without component failures, that permit unwanted functions to occur or that inhibit desired functions due to a current or energy flow along an unexpected route created by power supply cross-ties, unanticipated ground switch operations, etc.

2. *Sneak Timing*. An inappropriate subsystem response in the sequencing of signals. For example, mistimed signals can render useless an output of step signals the same way that faulty ignition timing can ruin the performance of an automobile engine.

3. *Sneak Indicators*. A false or ambiguous system status resulting from an improper connection, at assembly, or control of display devices. For example, a light could glow while the load it monitors is not activated.

4. *Sneak Labels*. Lack of precise nomenclature or instructions on controls or operating consoles that can lead to operator errors

5. *Sneak Procedures*. Ambiguous wording, incomplete instructions, lack of caution notes, and similar deficiencies that may result in improper action under contingency operations.

5-6.2 TECHNIQUE AND FORMAT

As indicated previously, the techniques and formats for conducting sneak analyses were developed by the Boeing Company. Papers providing much of the background of these techniques were presented at various professional meetings, including System Safety Society International Conferences. The information that follows has been taken from these papers—principally, Refs. 17 and 19.

The type of data used for the SCA technique is an important factor in providing the complete body of information required. Detail, as-manufactured-level draw-

ings—not schematics or functional drawings—are necessary to establish the data base. The SCA technique, therefore, uses controlling documentation that defines the "as built" or "as manufactured" configuration (Ref. 19). This statement that manufacturing drawings must be used does not contradict a previous statement in par. 5-6.1 which indicated an SCA should be initiated in the preliminary design stage. Here, gross configurations that could result in a sneak circuit can be discovered and eliminated; the detail drawings uncover the subtle sneak circuits.

5-6.2.1 Techniques

It has been proven that sneak circuits have distinct characteristics in all electrical systems. It is these telltale characteristics that enable formal analysis techniques to detect sneak potential in electrical hardware designs. The

formal analysis techniques for SCA incorporate two essential tasks, i.e., (Ref. 17)

1. Recognition of basic topological patterns inherent in all circuitry

2. Application of clues that have been found to characterize sneak circuit conditions.

Each of these essential tasks is discussed in the paragraphs that follow.

5-6.2.1.1 Topographical Patterns (Ref. 19)

The approach is referred to as "topological" in the sense that unswitchable power (unremovable) always is assumed to be at the top of a "tree" and unswitchable ground at the bottom. The SCA is based upon the postulate that all topological trees consist of one or more of the five possible topographs, illustrated in Fig. 5-17, that can be

**(A) Straight-Line Pattern
(No Nodes)**

**(B) Ground Dome
(Switched Ground-to-Ground Path)**

**(C) Power Dome
(Switched Power-to-Power Path)**

**(D) Combination Dome
(Combination Paths Through Node)**

**(E) Reverse Current Pattern
(Current Reverses Through Cross Branch)
(H-Pattern)**
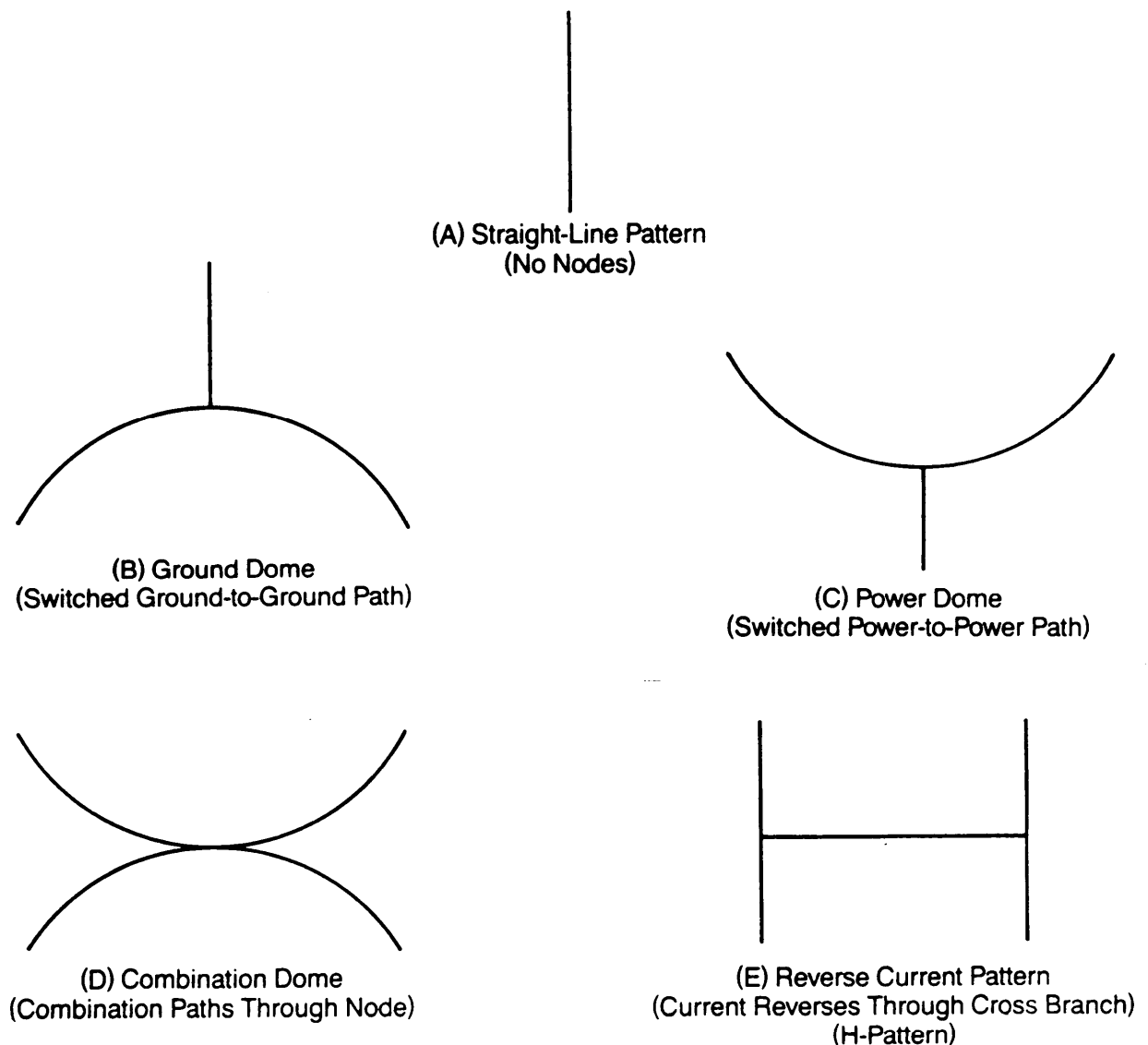
Figure 5-17. Basic Node Topographs (Ref. 19)

assessed for sneak potential at each node. The circuitry to be analyzed is redrawn in what is referred to as a "node-topograph" form. This method of circuit representation will reveal the topographical patterns characterizing the circuitry—i.e., ground dome, power dome, combination dome, or H-pattern—as illustrated in Fig. 5-17. One of

these patterns or several in combination will represent the subject circuitry. Fig. 5-18 is a schematic representation of a circuit to be analyzed for sneak circuit conditions. Fig. 5-19 shows the topological representation of Fig. 5-18. Although at first glance it may appear that this circuit is more complex than any of the basic patterns, a
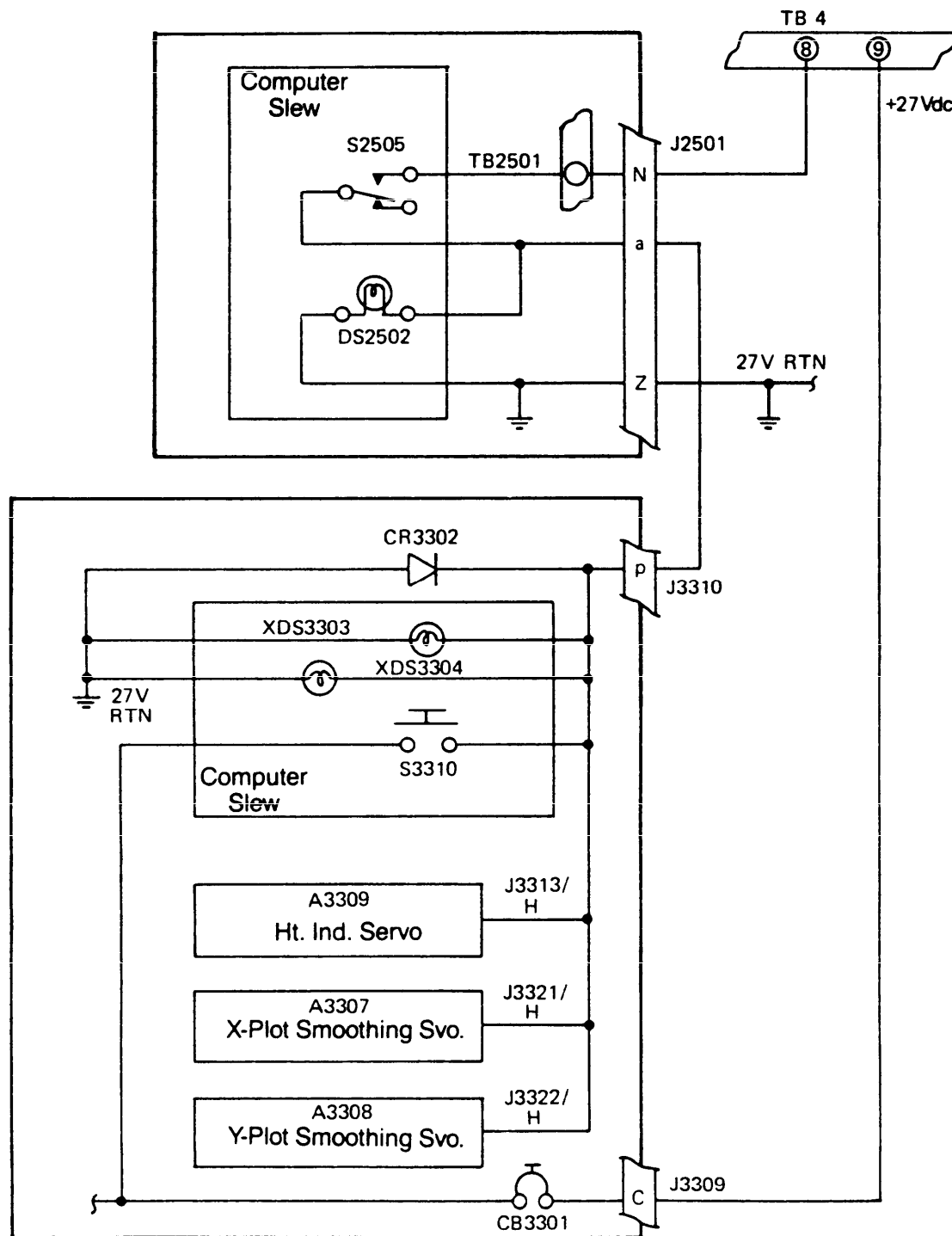
Figure 5-18.   Circuitry as Shown on Schematic to be Analyzed for Sneak Circuit (Ref. 19)
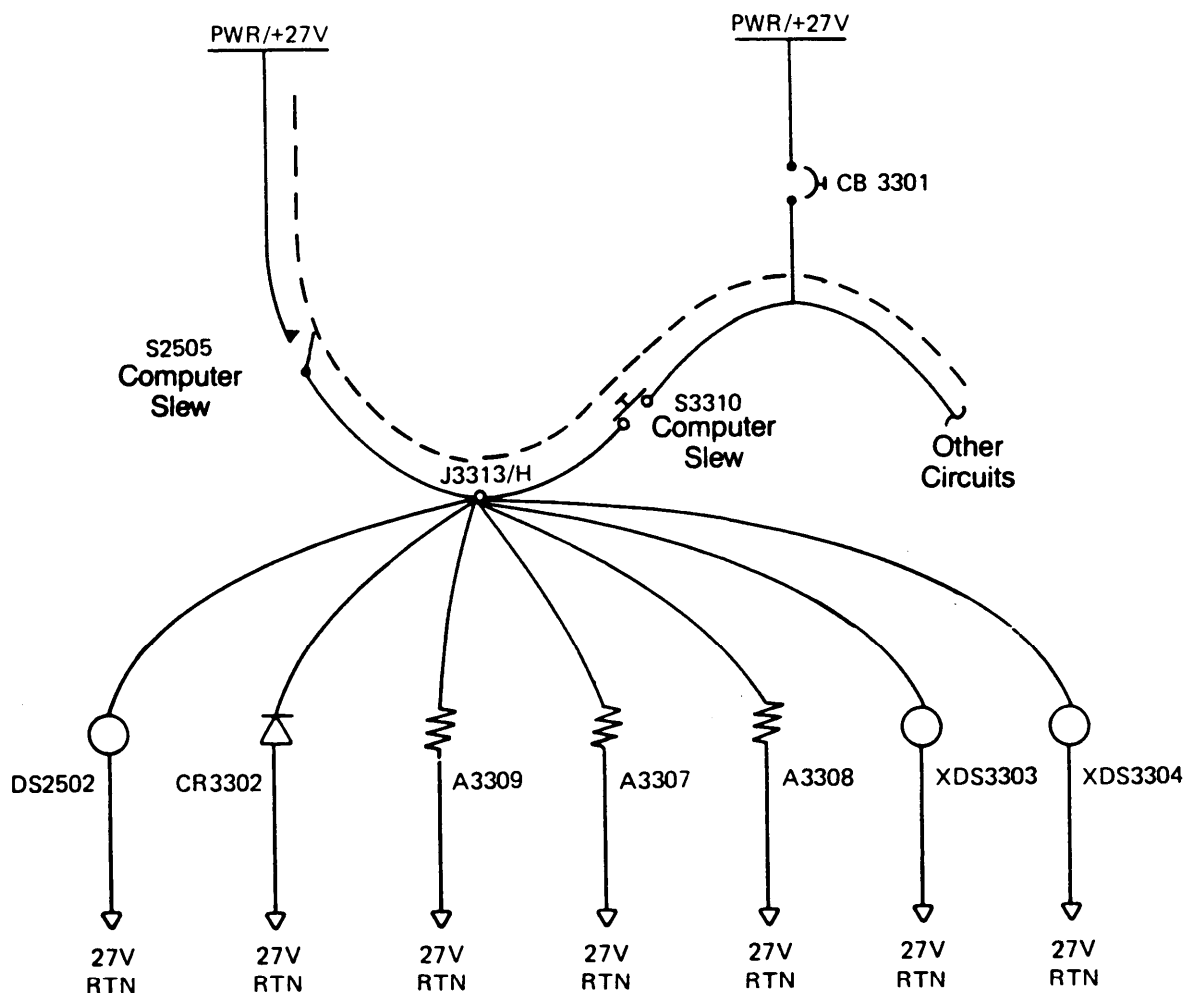
Figure 5-19. Network Tree Representation of Fig. 5-18 (Ref. 19)

closer inspection will reveal that it is a combination of these patterns. The fact that the circuits can be broken down into the basic patterns allows a series of clues to be applied for recognition of possible sneak circuit conditions. Clues are discussed in par. 5-6.2.1.2.

5-6.2.1.2 Clues (Ref. 19)

Clues are questions—suggested by the circuit topological representations (Fig. 5-17)—the analyst asks about the circuit to help identify combinations of controls and loads which are involved in all types of sneak circuits. The clues are standardized lists of questions—developed by companies with experience in using SCA—that assist the analyst in determining the different ways a given circuit pattern can produce a sneak condition. The list of questions is continually being expanded; most of the questions are held as proprietary information. For example, for a circuit represented by the "H" topograph (Fig. 5-17(E)), the list contains more than 60 clues. Simple examples, provided by the Boeing Company, of the node-topo-

logical/clue relationships are shown in Fig. 5-20 and Tables 5-2 and 5-3. The clues are learned best through application. The intent here was to indicate that an orderly approach exists for sneak potential identification in topological trees through a complete assessment of the topographs representing each node.

5-6.2.2 Format

Fig. 5-21 is an example of the form used to list data to be entered into the computer for processing. These computer data masterfiles form the data base for the computer-aided SCA. When all masterfiles are complete, a series of programs referred to as the "automated sneak program" (ASP) is run. The programs do two things:

1. All continuity data are searched by the computer, starting at the power points and terminating at ground, other power points, or at open ends.

2. The programs provide outputs that represent the continuity data in the masterfile.

Power

Ground

1. Do power and ground originate at same source?
2. Does power match the loads—i.e., AC, DC, signal, polarity, level, etc.?
3. Is switch S_1 open when load L_1 is desired?
4. Is switch S_1 closed when load L_1 is not desired?
5. Is switch S_1 necessary?
6. Does label of switch S_1 match function of load L_1?

Note: S_1 is a general switch—i.e., circuit breaker, fuse, etc.
   L_1 is a general load—i.e., logic gate output, relay coil, etc.

(A) Single-Line (No Node) Topograph

Power

Ground   **Ground**

General switches S_i represent any current interrupter, and general loads L_i have impedance from 0 to whatever limits are applied to the scope of the analysis. Each may represent the equivalent of many individual components in series as seen by node N within any given topological tree.

One sneak possibility of this pattern is obvious. If either ground is not the true return for power supply, then a distinct possibility exists that the grounds will be at different absolute potentials. Under this condition current can flow through L_2 and L_3, assuming S_2 and S_3 are closed, even if S_1 is open to remove power. A few of the more straightforward questions (clues) are

1. S_1 open: Is L_1, L_2, and/or L_3 desired?
2. S_2 open: Is L_2 desired (and inverse of S_1, S_2 closed; L_2 not desired)?
3. S_3 open: Is L_3 desired (and inverse)?
4. Does circuit loading through L_2 by-pass L_3 or inverse?
5. Does label of S_2 reflect true function of control for L_2 (same for S_3-L_3)?
6. Does label of S_1 reflect the function of only part of the circuit, e.g., L_2 and not L_3 or vice-versa?

These clues are not exhaustive—there are additional, more complicated ones. For example, L_2 could be an indicator required to monitor the operation of L_3. Yet, if S_3 is open (L_3 "off"), the indicator L_2 can falsely state that L_3 is "on".
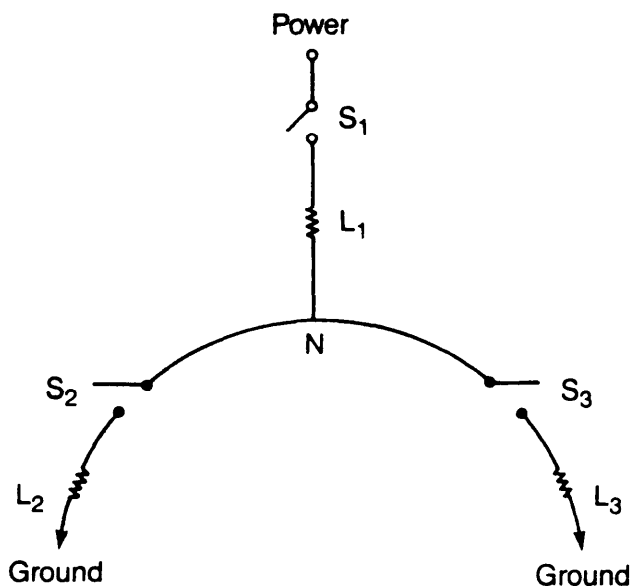
(B) Double Ground Node Topograph

Figure 5-20. Node Topograph/Clue Relationship (Adapted from Ref. 17)

Schematic   Detailed Circuitry   Combination Dome

Digital Clue:	Impact	Basic Clue:
Outputs tied together	Undefined logic	Undesired paths: S_1
Output controls must be	state on bus	to S_4 or S_3 to S_2
mutually exclusive		

(C) Combination Dome Topograph
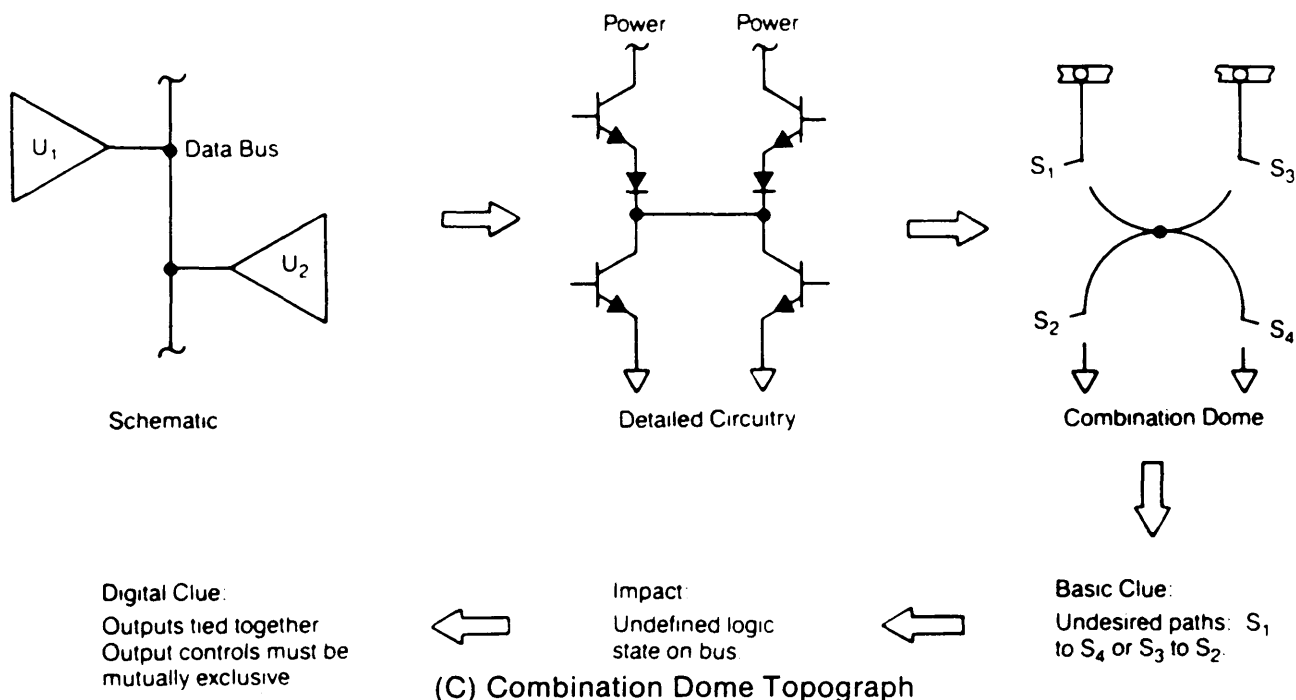
Figure 5-20. (cont'd)

Formats for output data are considered proprietary because the input they contain would permit programmers to determine the details of proprietary SCA programs. The format for a sneak analysis report is narrative and is illustrated by the example, Fig. 5-22, provided by the Boeing Company.

5-6.2.3 Guidelines

Guidelines for the application of the techniques follow:

1. Refer to other analyses—PHA, FMECA, or FTA—to identify the adverse end events that can result from sneak circuits. Review the equipment design to identify those circuits to be analyzed.

2. Mark the partition points where different subsystems and "black boxes" interface so that the overall analysis can be divided into manageable portions for detailed analyses.

3. Review the drawing of each black box, such as that shown in Fig. 5-18, which shows circuitry, components, and their interconnections. By use of standard electrical symbology, prepare the data from the "as built" drawings for computer processing. This will also provide an independent review of the completeness of design information for production purposes.

4. Uniquely identify and encode all wire segments. These data are entered into the computer. The information entered includes each and every signal path segment, using "From-To" identification, as shown in Fig. 5-21.

5. Process the data using an appropriate SCA software program such as ASP or Digital Analysis Program.

(These programs are proprietary, but some of them are available for sale.) The output of the computer-processed data will define all the possible paths that can exist in the circuitry.

6. By use of topological symbols (Fig. 5-17), prepare individual network "trees", as shown in Fig. 5-19. These trees use a representation different from those in standardized electrical drawings and show such factors as circuits that can receive power from designated points; power and ground points; and components—such as loads, diodes, switches, and umbilical disconnects—between power and ground points. Network trees can be drawn automatically by a computer-controlled plotter or manually on a graphics terminal by using the computer output data.

7. Prepare a network "forest" that is a representation of all the inputs required to cause each adverse end event, and the circuitry and units involved in the generation, control, and transmittal of those inputs. The "forest" diagram will show the interfaces between units (Fig. 5-23).

8. Apply sneak clues to identify and analyze sneak circuit paths. Par. 5-6.2.1.2 discusses clues.

5-6.3 SOURCES OF DATA

Data for the circuitry to be analyzed in a sneak circuit analysis can be obtained from wiring diagrams and lists, schematics, signal lists, parts lists, and interconnection drawings. For a final, rigorous SCA, however, "as built" drawings must be used.

TABLE 5-2.
SOME SAMPLE DIGITAL DEVICE CLUES

Latches

CLUE:	Output of latch goes off card, out of box, etc.
PROBLEM:	Signal reflections may reset the latch.
CLUE:	Asynchronous input data
PROBLEM:	Violation of setup/hold times may cause output hang-up.
CLUE:	Asynchronous clear or preset used for other than power on initialization
PROBLEM:	Clear/preset may occur as latch is clocked, which results in pulse (glitch) output.
CLUE:	Latch not initialized
PROBLEM:	Initial system stated undefined

Counters

CLUE:	Output of counter decoded with combinational (asynchronous) logic
PROBLEM:	Small differences in output transition time may be decoded into glitches.
CLUE:	Counter not initialized
PROBLEM:	Inaccurate count

TABLE 5-3.
EXAMPLE LOGIC CLUES

1. *Logic Loop With Odd Number of Inversions:*

Topology

Clue:

Boolean $B = A \cdot \overline{B}$

Problem: The loop trends to be stable, which results in a possible glitch or insufficient pulse width.

2. *Logic Splits and Rejoins:*

Topology

Clue:

Boolean $B = A \cdot \overline{A}$
$B = A + \overline{A}$
$B = A \cdot A$
$B = \overline{A} \cdot A$

Problem: a. Logic race may result in glitch.
b. Possible unnecessary logic.

Note: $\overline{A} \equiv$ not A
$\overline{B} \equiv$ not B

5-6.4   EXAMPLE

The SCA group at Boeing Aerospace Company stated that during the Army's PERSHING missile SCA contract, 20 sneak circuits, 12 design anomalies, and 40 drawing errors were found. Because SCA programs and outputs are proprietary, most information suitable for examples is not available to the general public. The example addressed is a sneak analysis report on the Army HELLFIRE missile that was provided by the Boeing Sneak Analysis Group (Fig. 5-22).

An example of applying clues in one of the intermediate steps in the sneak analysis example is given in Fig. 5-24. In Fig. 5-24 the sneak circuit report HFM-3 clues are shown at positions identified as "X : - ". These are related to the interfaces, the technology families, and the analog to CMOS transition. To apply clues, verify whether a problem exists by calculating whether required voltages at input to U-8 are always met—i.e., never between 3.6 and 8.4 V). Additional examples of clues applied to various

typical topographs are given in Tables 5-2 and 5-3 and in Fig. 5-20.

5-6.5   ADVANTAGES

Advantages claimed (Refs. 16, 17, 21, and 22) for SCA include

1. SCA is an effective technique when used to isolate problems that escape other methods of identification, such as identifying both intended and unintended operating conditions.

2. SCA can be used to assist in controlling the configuration of a subsystem, especially if numerous changes or modifications are occurring.

3. SCA is performed by analysts using computer programs that make an independent assessment of an entire subsystem—hardware, software, and interfaces—more thorough than the reviews done by design checkers.

4. Once the initial SCA has been done, it can be updated quickly to analyze the effects of modifications.

COMPUTER INPUT FORM

Black Box Detail Schematic

CARD TYPE	BOX REF DES	MODULE	SUBSYSTEM	DWG. NO.		PART NO.	BOX TITLE
					REV		
B1	702A2	A48	EPS	7623551	A	7623551 -1	MOT CONT

		FROM		TO		DIODE	IMP	REMARKS
		ITEM	PIN	ITEM	PIN			
B2	702A2	J1	A	SF10	1			
		SF10	1	SF10	2			15 AMP
		SF10	2	SK105	3			
		SK105	3	SK105	1			MOT CONT
		SK105	1	J1	B			
		J1	B	SK104	6			
		SK104	6	SK104	4			MOT CONT
		SK104	4	J1	C			

Figure 5-21. Example of Detail Schematic Encoding (Ref. 19)

5. The preparation of input information to the SCA reveals omissions in design documentation and aids in identifying errors in drawings.

6. SCA identifies mission-critical malfunctions frequently missed by the usual development and operational tests.

7. SCA provides functional diagrams down to component level.

8. SCA costs less than would the consequences of undetected problems.

5-6.6 LIMITATIONS

Limitations of SCA for safety purposes include

1. Every component and circuit must be included in the analysis. This all-inclusiveness makes the SCA expensive; however, it can be tailored or limited to specific high-risk subsystems or to those with potential hazards. Despite the cost, an SCA might be relatively inexpensive if it eliminates an event that could have catastrophic consequences.

2. SCA is usually conducted only after the design documentation has been completed. This factor makes the resulting design changes difficult and costly to imple-

ment. However, in some cases, the usefulness of the SCA for the identification of causes of costly problems in fielded materiel offsets this limitation.

3. SCA normally does not consider the effects that can result from the erroneous connections, short circuits, and human errors that—combined with potential design errors—constitute most circuitry problems. These areas of concern can be considered in a type of sneak analysis called common cause failure analysis (Fig. 5-25). If the "as built" drawings are in error, i.e., result in short circuits or wrong connections, an SCA will discover the errors.

4. SCA does not consider the effects of transient voltages, electromagnetic interference (EMI), and similar influences that can affect electronic systems. (This limitation also can be overcome by using a type of common cause failure analysis as illustrated in Fig. 5-25.)

5. The need to consider all combinations of switching positions, transients, and timing may require so much computer capability that the use of SCA for digital logic circuits may be impracticable.

6. For review of the topological sets, the clue lists have been developed from more than 10 yr of experience and are generally not available to designers.

SNEAK CIRCUIT REPORT HFM-3
HELLFIRE MISSILE

TITLE "G BIAS COMMAND" SIGNAL LEVEL IS
INDETERMINATE

DATE _____

ENGINEER _____

REFERENCES

1. U.S. Army MIRACOM Dwg. No. 13042343, Basic "Schematic Diagram-Scan and Mode No. 1".
2. U.S. Army MIRACOM Dwg. No. 13042203, Basic, "System Schematic".
3. U.S. Army MIRACOM Dwg. MOOTMS, "Telemetry Missile Schematic".
4. Rockwell International Dwg. V104—50151, Rev. A, "Autopilot Interconnect".
5. Rockwell International Dwg. V104—50153, Rev. A, "Autopilot Logic Module".
6. "COS/MOS Integrated Circuits" by RCA Corporation, 1977.

MODULE/EQUIPMENT — LOGIC MODULE, AUTOPILOT ASSEMBLY

EXPLANATION

Figure 1 shows the circuitry implementing the "G BIAS CMD" signal. Due to presence
of zener diode VR9, the voltage at pin P1/V is approximately 4.5 volts. This means
that the voltage at U7 pin 10 is given by : $2 \cdot (.6) V_{P1/V} = 5.4$ VDC (note that the out-
put of the ground compensation circuit is ≈ 0VDC). It follows that if the voltage at

voltage at U7 pin 1 = 5 VDC is greater than the voltage at U7 pin 2 = 2.7 VDC).
When the voltage at U7 pin 12 is −11 VDC then the voltage at U8 pin 8 is 0.5 VDC.
When the voltage at U7 pin 10 is 5.4 VDC, the voltage at U8 pins 5 & 6 is 5.4 volts.
Reference 6 (page 52) shows that: V_{IL} (MAX) = 3 volts (for V_{DD} = 10v) and = 4 volts
(for V_{DD} = +15 volts, V_{IH} (MIN) = 7 volts (for V_{DD} = 10V) and = 11 volts (for V_{DD} =
+15v). In the case where V_{DD} = 12 volts, it may be assumed that V_{IL} is between 3 and
4 volts and V_{IH} is between 7 and 11 volts.
Since 5.4 volts meets neither of these conditions, the output level (Hi or Lo) at
U8 pin 4 is indeterminate. This implies that the output level at U8 pin 10 ("G BIAS
CMD") is indeterminate, i.e., the low at pin 8 is not sufficient to determine the state
of the output.

POTENTIAL IMPACT

Inhibited functioning of the pitch integrator circuit, resulting in inaccurate missile
guidance commands.

RECOMMENDATION

Remove resistor R7 from the circuit. Disconnect pin 4 of U8 from pin 9. Connect U8
pin 9 to U8 pin 8 and tie pins 5 & 6 of U8 to ground. The circuit shown in Figure 2
will output as the circuit in Figure 1 with the exception that in the case of the laser
seeker G BIAS CMD will be high, not indeterminate.

CONTRACTOR ACTION BY _____   DATE _____

REMARKS

(A) Narrative Report

Figure 5-22.   Sneak Circuit Report HFM-3
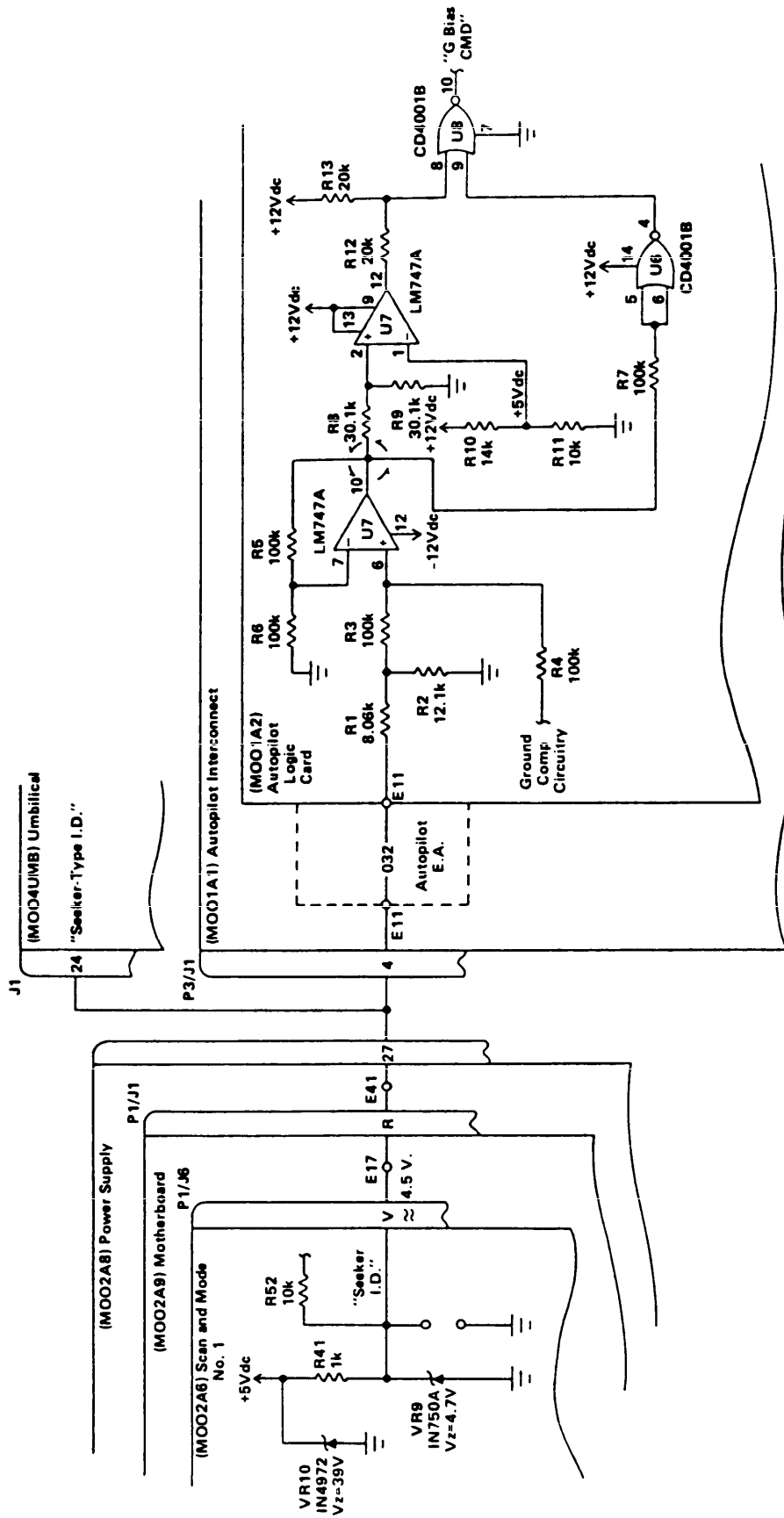
(B) "G Bias CMD" Logic

Figure 5-22. (cont'd)
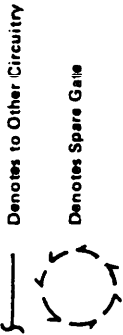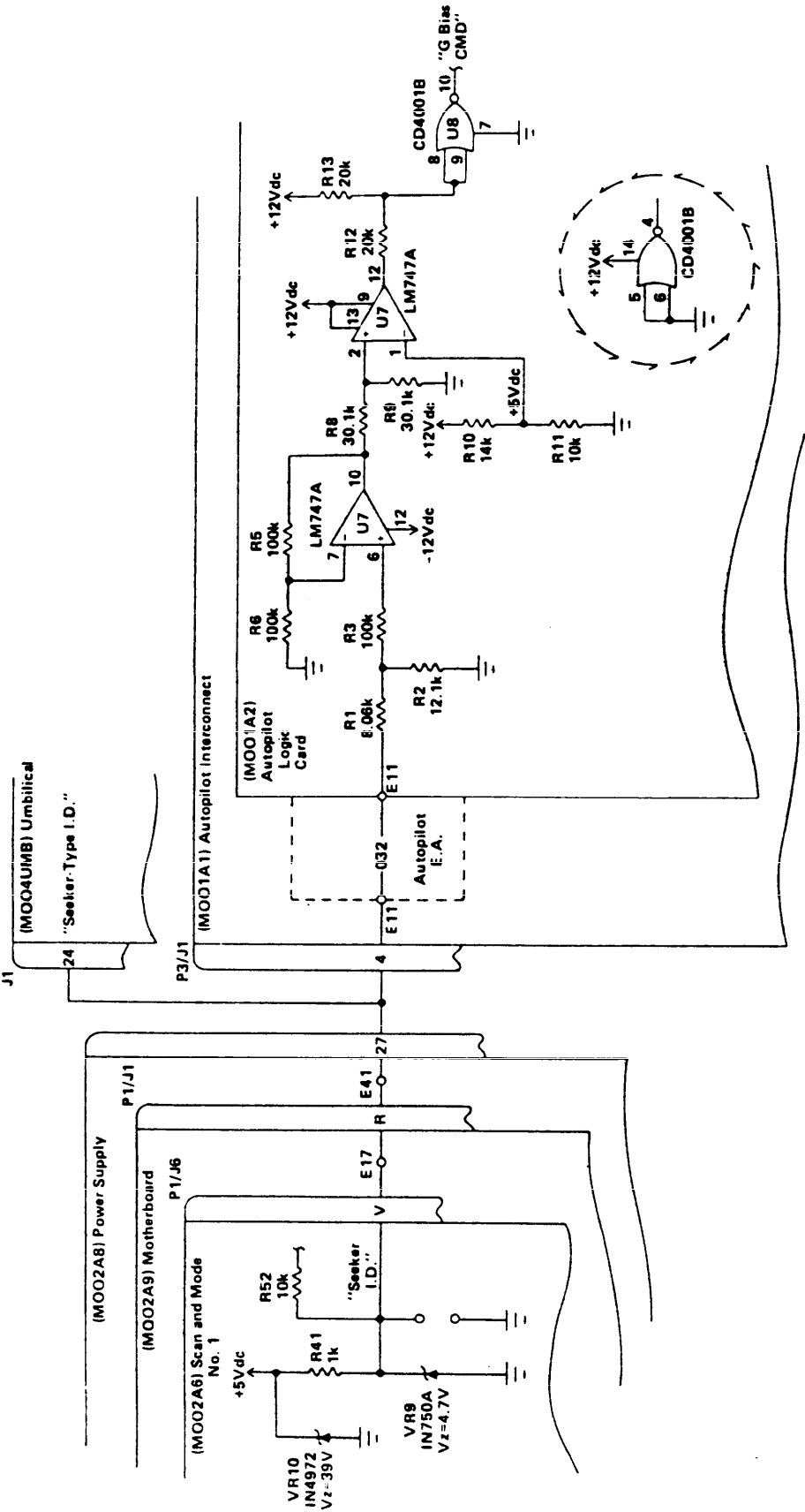
(C) Recommended Correction

Figure 5-22.   (cont'd)
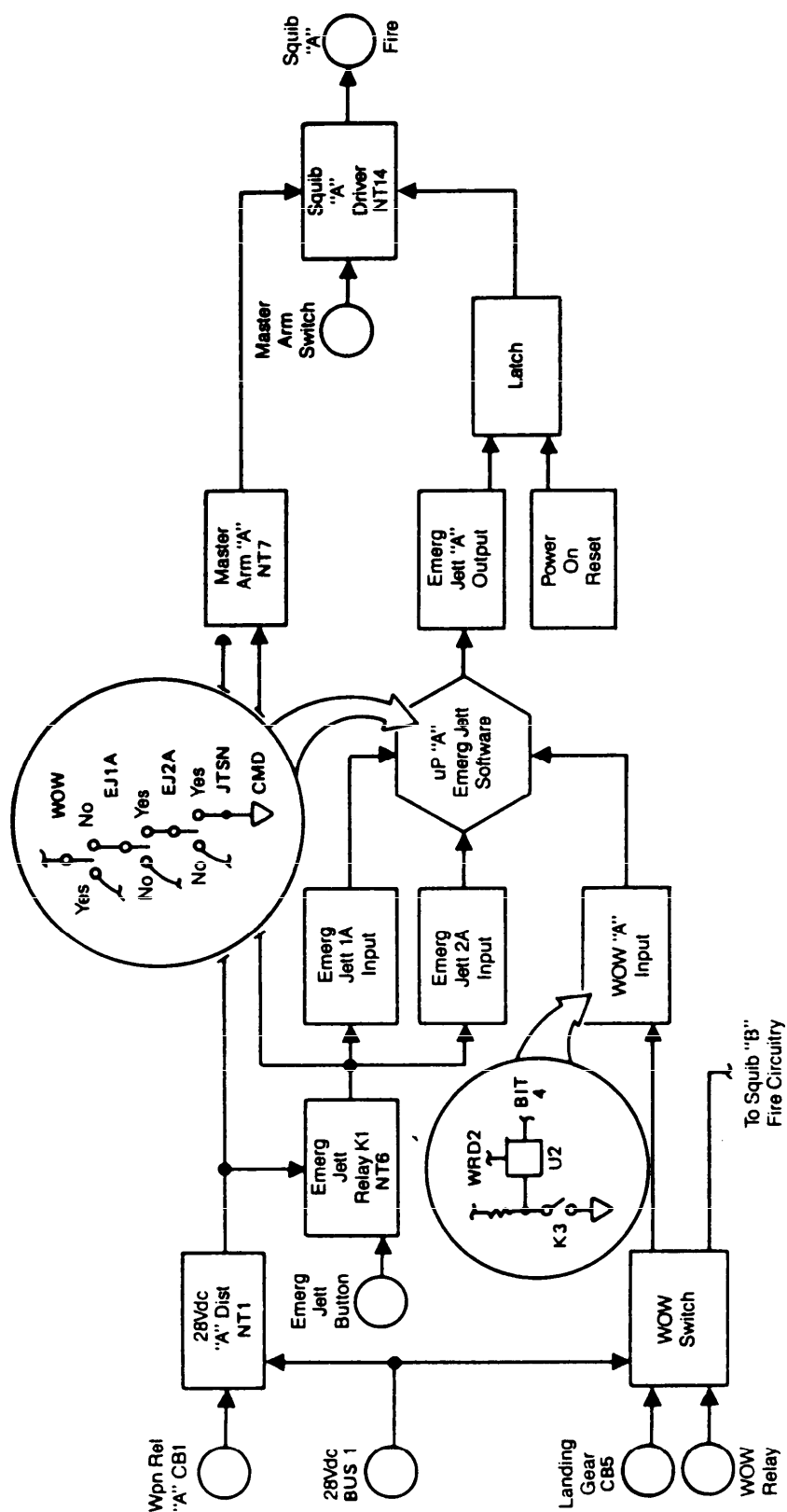
Figure 5-23. "Forest" for Squib Circuit (Ref. 20)
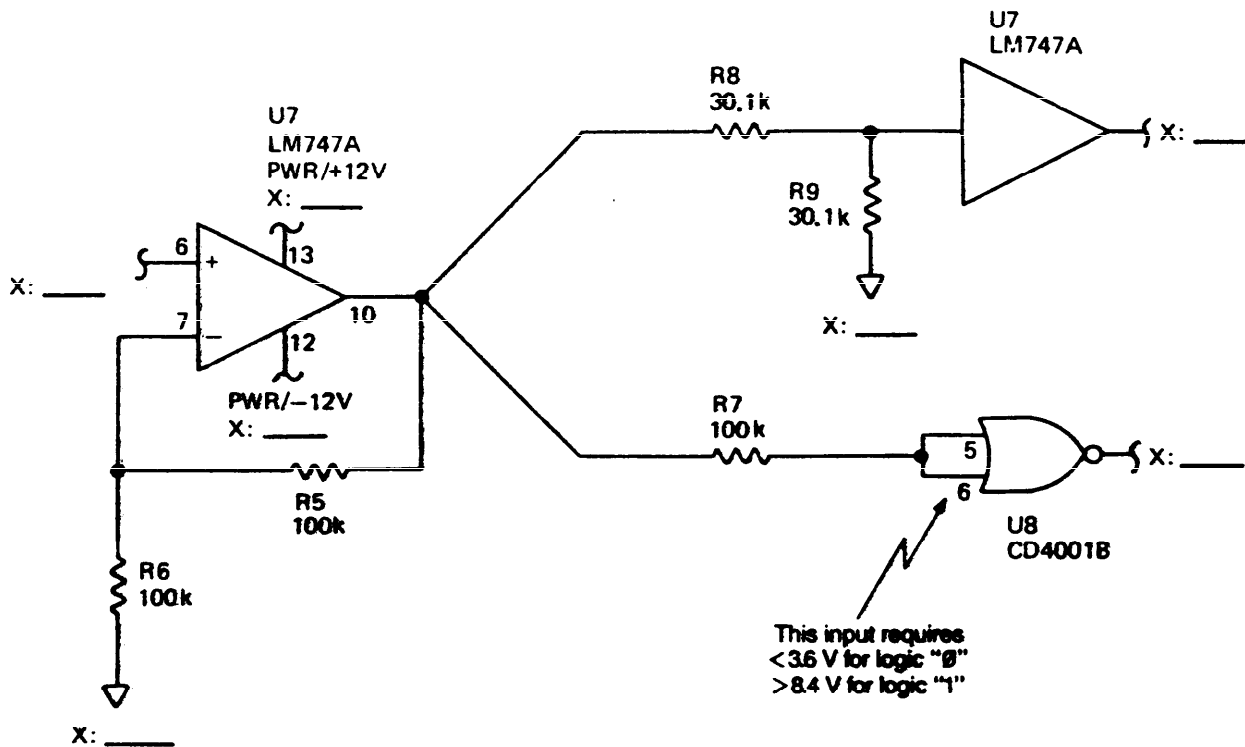
Figure 5-24.Application of Clues to Analog to CMOS Portion of Example Network of Fig. 5-22(B)
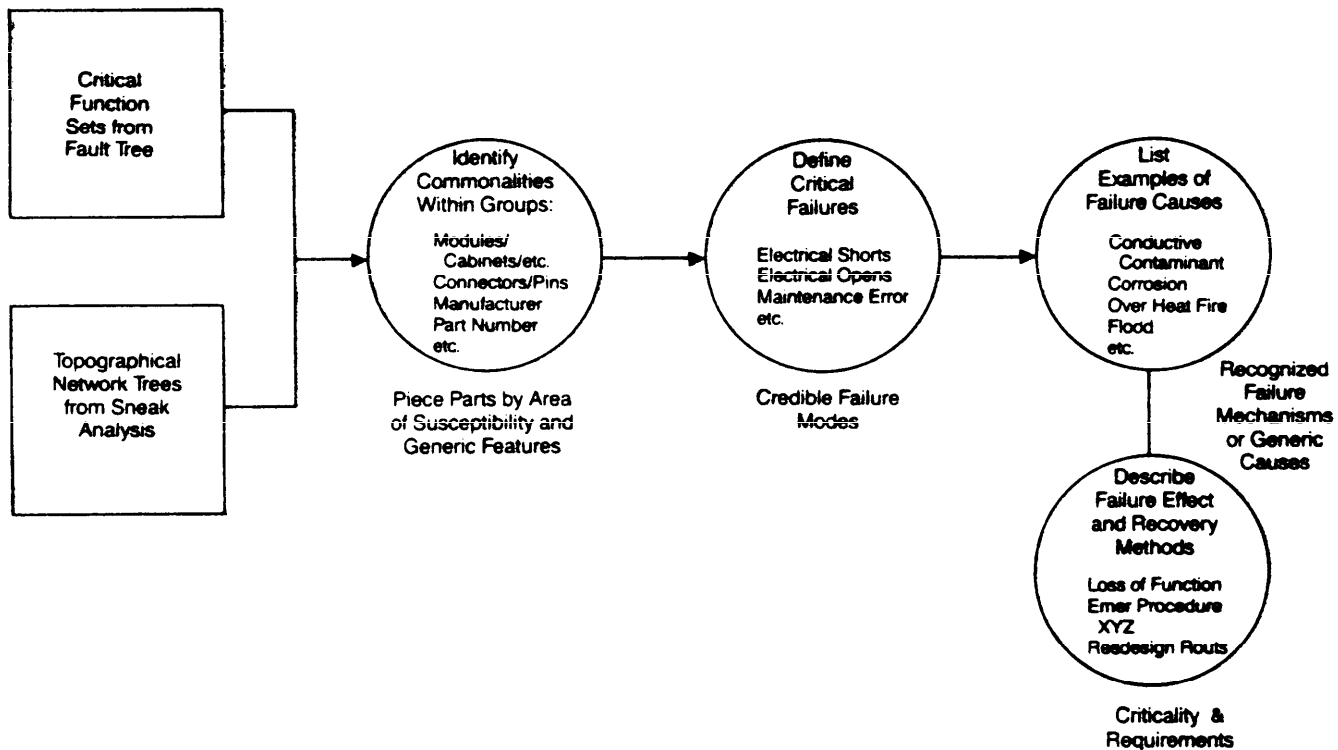
Figure 5-25.   Common Cause Failure Analysis (Ref. 20)

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

2. DI-SAFT-80101, *System Safety Hazard Analysis Report*, 20 January 1986.

3. ARP 962A, *Fault Failure Analysis Procedure*, SAE Aerospace Recommended Practice, Warrendale, PA, November 1979.

4. MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, 28 November 1984.

5. MIL-STD-785B, *Reliability Program for System and Equipment Development and Production*, 15 September 1980.

6. Willie Hammer, *Handbook of System and Production Safety*, Prentice-Hall, Englewood Cliffs, NJ, 1972, p. 158.

7. H. E. Arnzen, *Failure Mode and Effects Analysis: A Powerful Tool for Component and System Optimization*, Annals of Reliability and Maintainability Conference, 1966.

8. MIL-HDBK-217D, *Reliability Prediction of Electronic Equipment*, 13 June 1983.

9. *Nonelectronic Reliability Notebook*, RADC-TR-75-22, Rome Air Development Center, Air Force Systems Command, Griffis Air Force Base, NY, January 1975.

10. MIL-S-19500/533A, *Semiconductor Device, Diode, Silicon, Zener, Voltage Regulator, Solid Glass Noncavity Construction*, 25 March 1985.

11. Willie Hammer, *Product Safety Management and Engineering*, Prentice-Hall, Englewood Cliffs, NJ, 1980.

12. A. B. Mearns, *Fault Tree Analysis, The Study of Unlikely Events in Complex Systems*, Bell Telephone Laboratories, System Safety Symposium Proceedings, Seattle, WA, 8-9 June 1965, p. 1-14.

13. N. H. Roberts, D. G. Haasl, W. E. Vesely, and F. F. Goldberg, *Fault Tree Handbook*, NUREG-0492, US Nuclear Regulatory Commission, Washington, DC, March 1980.

14. TOP-3-2-504, *Safety Evaluation of Hand and Shoulder Weapons*, US Army Test and Evaluation Command, Aberdeen Proving Ground, MD, 1 March 1977.

15. S. A. Lapp and G. J. Powers, "Computer-Aided Synthesis of Fault Trees", IEEE Transactions on Reliability, VR-26, 1, 2 (April 1977).

16. W. F. Larsen, *Fault Tree Analysis*, Technical Report 3822, November 1968, Revised and reissued as Technical Report 4556, Picatinny Arsenal, Dover, NJ, January 1974.

17. J. P. Rankin, *Sneak Circuit Analysis*, Proceedings of First System Safety Symposium, July 1973, pp. 462-82.

18. SB08-P-108, "Plan, Apollo Spacecraft Sneak Circuit Analysis", Contract No. NASW-1650, National Aeronautics and Space Administration, March 1968, p. 1.

19. E. J. Hill and L. J. Bose, *Sneak Circuit Analysis of Military Systems*, Proceedings of Second System Safety Conference, July 1975, pp. 351-72.

20. P. D. McRae, Jr., *Sneak Analysis and System Safety, The Fit and Benefit*, Boeing Aerospace Company, Fifth International System Safety Conference, Denver, CO, 27-31 June 1981, pp. 1-11.

21. *Sneak Analysis*, Boeing Aerospace Co., Houston, TX, 1981.

22. *The General Dynamic System for Sneak Circuit Analysis*, General Dynamics, Convair Division, San Diego, CA, June 1980.

BIBLIOGRAPHY

NAVORD OD 44942, *Weapons System Safety Guidelines, Part III*, Naval Ordnance Systems Command, Department of the Navy.

K. P. Nelson, *The Outline and Use of System Safety and OSHA Compliance Guides for Use in Designing Equipment*, US Army Materiel Command, Alexandria, VA, April 1975.

F. Mazzill et al., *RADC Reliability Handbook*, 1, Technical Report No. RADC-TR-67-108, Rome Air Development Center, NY, November 1968.

G. Chiernowitz et al., *Electromechanical Component Reliability*, RADC-TDR-63-295, Rome Air Development Center, NY, May 1963.

J. Bauer et al., *Dormancy and Power On-Off Cycling Effects on Electronic Equipment and Part Reliability*, RADC-TR-73-248, Rome Air Development Center, NY, August 1973.

Keith Henney and Craig Walsh, Eds., *Electronic Components Handbook*, McGraw-Hill Book Co., New York, NY, 1957.

BIBLIOGRAPHY (cont'd)

W. Yurkowsky, *Data Collection for Nonelectronic Reliability Handbook*, (NEDCO I and NEDCO II), RADC-TR-68-114, Rome Air Development Center, NY, June 1968.

W. Yurkowsky, *Nonelectronic Reliability Notebook*, RADC-TR-75-22, Rome Air Development Center, NY, January 1975.

R. W. Burrows, *Long Life Assurance Study for Manned Spacecraft Long Life Hardware*, IV, N73-23856, Martin-Marietta Corporation, Denver, CO, September 1972.

K. K. Arora and H. C. Edfors, *Automated Production System Safety*, Proceedings 1975 Annual Reliability and Maintainability Symposium, p. 531-7, 1975.

AFSC DH 1-6, *System Safety*, Aeronautical Systems Division, Air Force Systems Command, April 1979.

Phase II Safety Study Report, Minuteman Launch Control System, Bell Telephone Laboratories, Whippany, NJ, May 1964.

Expansion of Scope for Minuteman Wing VI Fault Tree Analysis—A Feasibility Study, The Boeing Company, September 1964.

System Safety Engineering Analysis Techniques, The Boeing Company, September 1966.

System Safety Analytical Technology—Fault Tree Analysis, D2-113022-2, The Boeing Company, February 1970.

The Fundamentals of Hazard Analysis, SC 68-791, North American Rockwell Corporation, November 1968.

R. E. Barlow and F. Proschan, *Importance of System Components and Fault Tree Events*, University of California, February 1974.

R. E. Barlow and P. Chatterjee, *Introduction to Fault Tree Analysis*, University of California, December 1973.

L. Bass, H. W. Wynholds, and W. R. Porter, *Logic Tree Analysis—A Fault Tree Graphics Approach*, Lockheed Missiles and Space Company, August 1974.

R. G. Fussell, "How to Hand Calculate System Reliability and Safety Characteristics", R-24, IEEE Transactions on Reliability, August 1975.

J. A. Cannon, *A Complete Algorithm for Fault Tree Analysis*, Texas A&M University, College Station, TX, December 1970.

P. O. Chelson, *Reliability Computations Using Fault Tree Analysis*, Technical Report 32-1542, Jet Propulsion Laboratory, Pasadena, CA, December 1971.

J. B. Fussell, *Review of Fault Tree Analysis With Emphasis on Limitations*, CONF-750860-1, Aerojet Nuclear Company, Irvine, CA, 1975.

J. B. Fussell *et al.*, "Fault Trees—A State-of-the-Art Discussion", R-23, IEEE Transactions on Reliability, April 1974.

E. L. Holt, *Likelihood Models*, First International System Safety Society Symposium, pp. 352-80, July 1973.

H. Lambert, *Fault Tree Analysis: An Overview*, Lawrence Livermore Laboratory, Livermore, CA, August 1974.

E. P. Lynch, *Introduction to Fault Tree Synthesis Using the Lapp-Powers Methodology*, ANL/EES-CP-3, Argonne National Laboratory, 1978.

S. W. Malasky and P. J. Tregarthen, *An Improvement in Cut and Path Set Determination*, 1980 Proceedings Annual Reliability and Maintainability Symposium, pp. 367-73, 1980.

J. Pauperas, Jr., *Guidelines for Fault Tree Analysis*, D02384, TRW, Redondo Beach, CA, October 1978.

D. R. Pleas *et al.*, *Apollo Logic Diagram Analysis Guideline*, M70-34384, The Boeing Company, June 1968.

W. E. Vesely, *Analysis of Fault Trees by Kenetic Tree Theory*, IN-1330, Idaho Nuclear Corporation, October 1969.

W. E. Vesely and R. E. Narum, *PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree*, IN-1349, Idaho Nuclear Corporation, August 1970.

R. R. Willie, *Computer-Aided Fault Tree Analysis*, University of California, August 1978.

Fault Tree Construction Guide, Armament Development and Test Center, Eglin Air Force Base, FL, May 1974.

S. J. Calvillo, *Verification of Hardware/Software Integration Through Sneak Analysis*.

J. Browne, Jr., *Benefits of Sneak Circuit Analysis for Defense Programs*, Proceedings of the Third System Safety Conference, pp. 303-20, October 1972.

R. C. Clardy, *Sneak Analysis: An Integrated Approach*, Proceedings of the Third System Safety Conference, pp. 377-87, October 1977.

CHAPTER 6
SYSTEM HAZARD ANALYSIS

The subsystem interface relationships that make up the system are discussed under the subheadings physical, functional, and flow. System hazard analysis methods and techniques are defined together with several specific supporting techniques such as plotting of hazards and human error analysis. Sources of data for system hazard analyses are given, and the advantages and limitations of the various techniques are stated. Data are provided on formats for conduct of the system hazard analysis.

6-1 DESCRIPTION AND PURPOSE

This chapter presents detailed information on the system hazard analysis (SHA) discussed in MIL-STD-882 (Ref. 1) and Data Item Description (DID) DI-SAFT-80101 (Ref. 2). The SHA is necessary to define the safety interfaces between subsystems and to identify possible safety hazards in the overall system. It will determine whether system hazards can be eliminated or controlled with design safeguards. The need for procedural safeguards, however, will be recommended only as a last resort.

That certain of the hazards inherent in the overall system will result from hazards inherent in the subsystems is quite evident. What is not so evident is the manner in which the subsystem safety problems may affect the system as a whole. One example of this involves a self-propelled gun. During development the engine is tested and found to have a vibration mode that falls just within acceptable limits. The hydraulic pumps and electric generator (or alternator) are tested separately and found acceptable. When the engine is tested with the pumps and generator, the vibration mode grows worse and becomes an unacceptable hazard. However, when the engine and all engine-driven equipment are mounted in the self-propelled gun and the complete system is tested, it might exhibit better or worse vibration characteristics than the subsystems. The point is that the SHA, either from dynamic analysis or test data, can provide results quite different from what might be expected from a simple compilation of subsystem hazard analyses (SSHAs) because of the interactions of the individual subsystems.

In addition, a system as a whole can present a more hazardous situation than that found in the subsystems. Consider a rifle, for example. The combination of the rifle and the ammunition is a much more hazardous (lethal) system than that represented by either of the subsystems.

Thus SHA analyzes the effect that each subsystem has on all others during the normal and abnormal operation of each one, but, more importantly, it analyzes the operation of the system as a whole. The SHA must establish that separate units and subsystems can be integrated into

a safe system. The operation of one unit or subsystem must not impair the safe performance of, or cause damage to, another unit or subsystem within the system. Because human reactions required for normal system operation are considered part of the system, "human error" must be considered as a possible failure mode in the SHA. Lastly, the environment will have an effect on the system and must also be considered in the SHA.

In summary, the value of an SHA lies in its identification of

1. Interface problems
2. Dependent failure problems
3. Synergistic hazards
4. Additive hazards.

When a safety level has been defined for a specific system, proof that the design satisfies that safety requirement can be obtained only by preparing an SHA. Other safety analyses, studies, test reports, experience with related systems, and program data—such as reliability reports—will be useful to support the SHA.

6-1.1 INTERFACES

The various interface relationships among the units or subsystems that must be considered in the SHA can be categorized principally as physical, functional, or flow relationships. Each is discussed in the paragraphs that follow.

6-1.1.1 Physical Relationships

Each subsystem might be well designed and built, and it may operate as required when tested separately. However, when the subsystems are combined into a system, they may not fit together because of dimensional incompatibility or together they may create other physical difficulties leading to possible safety hazards. Examples follow:

1. The clearance between units is so small that one or more units can be damaged when a unit is being removed or replaced during a maintenance operation.

2. Access to, or egress from, equipment may be impossible or restricted because of dimensions or placement of a unit within the equipment.

3. Inability to tighten, join, or mate units that should fit tightly together can result in structural failures. It may be impossible to prevent movement between two parts because of bolt holes of different sizes or a convex surface is being mated with a flat surface.

4. Units or subsystems may have symmetrical mounts and at least two duplicate hydraulic, pneumatic, or electrical connectors that create the probability of installation and connection errors. From a system safety standpoint, the mating process must be such—e.g., the use of differently sized and shaped connectors—that assembly and connection errors will be impossible, have an extremely low probability of occurrence, or will not lead to a safety problem if a mistake is made.

5. Moving parts, if left unguarded, may be hazardous to operating personnel.

6. A vehicle filter that is difficult to remove may not be cleaned or changed as required. Thus the filter may clog or the subsystem may fail due to contamination, which would result in a mission failure of the system.

7. The physical location of a subsystem may create a potential system hazard. A vehicle fuel subsystem with fuel lines routed very near a hot exhaust manifold may cause the volatile fuel in the line to vaporize; this results in "vapor lock" and fuel starvation.

8. Tolerance buildup among several subsystems that individually meet their tolerance requirement may result in failure to assemble properly.

6-1.1.2 Functional Relationships

The output of one subsystem may be the input to an interfacing subsystem, or it may control the output of the interfacing subsystem. Unless the output is correct during a given time frame, it may damage the interfacing subsystem and constitute a possible system hazard. Typical problems that could occur are

1. *Zero Output.* The output of the subsystem fails completely, so the receiving subsystem does not receive the necessary input from the upstream subsystem. This could be caused by an internal malfunction in the upstream subsystem or an interconnect failure. For example, a missile may become out of control because of reduced input to the flight control subsystem.

2. *Degraded Output.* A partial failure occurs, and a downstream subsystem does not receive sufficient input. For example, partial clogging of hydraulic or pneumatic passages can reduce flow so that a downstream unit is inadequately supplied with fluid pressure or volume. This can cause reduced pressure or cooling effects and can result in inadequate lubrication, reduced braking, overheating, jamming of automatic feed mechanisms, and similar deficiencies.

3. *Excessive Output.* A radar may be damaged because the output voltage and current of a power supply were not regulated. Vehicle batteries have been damaged

from overcharging due to failure of the voltage regulator. Failure of the reverse current relay can cause the battery to provide high current to a generator when the engine is stopped and thus burn out the generator.

4. *Erratic Output.* Intermittent or unstable operation can cause relays or valves to chatter, which results in surges of electric power or fluid flow. Cavitation within a torque converter may cause damaging power surges.

5. *Unprogrammed Output.* Inadvertent operation or an erroneous output could be a hazard if it caused damage to interfacing subsystems. Inadvertent activation has also caused injuries to operating personnel. For example, if an interlock between a hatch cover and a tank turret fails, the turret could be rotated while someone stood in the hatch, and the turret could strike the person.

6. *Undesirable Side Effects.* Although the programmed outputs of a subsystem are within prescribed limits, they may generate other outputs that could be damaging. An electrical subsystem or unit may generate heat that could damage nearby equipment. The scavenger pressure of one pump may damage a redundant pump, which would result in total failure of the system. Laser devices may cause injury when laser energy is reflected by specular surfaces into the eyes of unprotected persons.

6-1.1.3 Flow Relationships

Military systems use many forms of energy in various functional relationships to accomplish a mission. When this energy—electrical, mechanical, thermal, nuclear, chemical, or whatever—is maintained in its normal, controlled state in a system, it is useful to the mission. If the energy becomes uncontrolled, it not only can jeopardize the mission, but it can also harm personnel and damage equipment. One method of examining the potential hazard of energy "flows" in a system is to examine all energy sources and how they normally flow and what possible abnormal flows could occur.

The flow of energy between subsystems generally is designed to occur in a "closed system" such as in piping or wiring. Other energy flows may be "unconfined"; for example, most equipment heats up during operation and will radiate heat energy from one subsystem to another. RF energy purposely is radiated in communications and radar operations and may have an effect on other systems, subsystems, or personnel. Review of these flow relationships and possible failure modes is important for identifying possible system hazards. Some potential energy flow problems and effects are

1. *Connections between two units may be faulty.* The lack of adequate bonding when mounting radar antenna waveguides may result in the escape of RF energy above acceptable levels in personnel areas.

2. *Interconnection may fail completely.* High-pressure hoses can burst when inadvertently overpressurized. Such failures cause hoses to whip violently and injure

persons and damage equipment within their range. If the fluid is hazardous—e.g., hot, toxic, etc.—additional hazards occur.

3. *Interconnections can suffer a partial failure.* Leakage of fluid or gas can occur at a break in the line itself or at the interconnection between the line and the unit. The loss of fluid or gas can result in a loss of pressure or in contamination of work areas, materials, and nearby equipment. Toxic material that escapes under high pressure can act as a fluid needle or knife and can penetrate the skin to cause septicemia. A small leak of combustible liquid under high pressure could atomize and cause a fire or explosion if exposed to an ignition source. If the line contains a hazardous fluid, even a small leak may prove highly damaging or dangerous. A small leak near an engine can cause fuel to hit the hot exhaust manifold and cause a fire. Safety analysts, therefore, must consider all adverse characteristics of each fluid used in a system.

6-1.2 METHODS OF ANALYSIS

Most of the methods of analysis described in previous chapters can be used for SHA. However, in an SHA, these same methods of analysis require a shift in the safety viewpoint. Instead of considering the hazards to lie solely within each of the separate subsystems that comprise the system, the analyst must now consider hazards that exist because of the interactions of these same subsystems and their functioning as a system entity.

A system-level fault hazard analysis (FHA) starts with a known hazard such as a vehicle out of control. The FHA then attempts to discover where in the system the potential for the hazard exists—such as in the brake or steering subsystems—and determines what type of undesired end events it may lead to, e.g., the crashing of the vehicle into objects or people. Ref. 3 discusses other aspects of analysis methodology.

A system fault tree analysis (FTA) starts with an undesired end event—such as the crashing of a vehicle into things or people—and analyzes the system to determine whether and how it may occur. Failures of specific subsystems such as the brake and steering subsystem will be identified by this method of analysis.

These examples regarding the use of an FHA or an FTA underline the fact that the methods of analysis are not necessarily different in all respects. The method(s) selected for a particular SHA will depend on the level of available information about the system, the acquisition time frame, and the end use of the SHA. An SHA for use by program managers may take one form; an SHA for use by engineers that quantifies the safety level may take another form and require a different method. In the interest of time and economy, however, an effort should be made to adopt a method that will satisfy multiple users.

The system-level failure mode, effects, and criticality analysis (FMECA) usually tries to determine the effects that specific failure modes of individual components can have on operations of the entire system. A system software analysis, described in Chapter 7, also involves considerations of how an entire system can be affected by one subsystem, e.g., a computer. The possibility of human error can be considered in either of these methods of analysis. When a human operation of some type is identified as a potential failure in the chain of events leading to the undesired event (because the human can make an error), the probability that the person will make the error should be included in the SHA. (See par. 6-2.2.6.2.)

Selected outputs of the SSHA are considered as candidate inputs to the SHA. In addition, as more is learned about the system, the possibility of a new undesired event may need investigation. If the possible cause of this newly identified, undesired event is identified as a subsystem event, the SSHA will require updating. For this reason, all safety analyses should be performed iteratively according to the on-going requirements of the program. Like good wine, analyses just may improve with age.

The SHA can also employ information generated in the preliminary hazard analysis (PHA). (See Chapter 4.) The PHA is particularly valuable for this purpose because it generally covers the entire system and is intended to identify all potential hazards. It is also intended to optimize safety by establishing optimum design requirements within the constraints of operation requirements, schedules, and resources. The SHA should include a review of those system and mission hazards identified in the updated PHA and a review of the interrelationships of the various subsystems.

6-2 ANALYSIS FORMAT AND TECHNIQUE

The analyses described in this chapter will place the emphasis on the interrelationships between the subsystems for

1. Compliance with safety criteria

2. Possible independent, dependent, and simultaneous failures, including those of safety devices, that could present a hazardous condition

3. Possible damage to one subsystem from normal operation or failure of another subsystem.

6-2.1 FORMATS

The format for the SHA should be selected for compatibility with the analysis method(s) to be employed, which in turn should be selected to satisfy the requirements of the particular system development program. If there is a program need for an SHA during the early design phases of a large system, the SHA can be presented in a narrative format described in par. 4-3.1.2. This is usually done to assist in formulating design criteria and emphasizing the problem areas. Whether the analyst should do a PHA or

an SHA at this time will be a decision influenced by program factors such as the use for the SHA and the schedule for updating the PHA. The basic formats for the SHA are the diagrammatic format such as that for the fault tree and the tabular format such as that for a fault hazard analysis. Each format has a somewhat different scope with its own primary objectives, advantages, and limitations discussed in pars. 6-5 and 6-6.

The selection of the correct format—that will result in the systematic completion of an analysis for a specific materiel acquisition program—will be helpful for obtaining a comprehensive and thorough assessment. The exact construction of the format to be used should be consistent with the particular needs and situations associated with the design to be evaluated. Fig. 6-1 is an example of a typical SHA tabular format that can be modified to satisfy various materiel acquisition program needs.

6-2.2 TECHNIQUES

The techniques of analysis used in preparing a system hazard analysis are primarily those used in the subsystem hazard analysis described in Chapter 5. Though the techniques are the same, remember that the safety viewpoint is now on the system rather than on the subsystem, as stated in par. 6-1.2. The methods of analysis for conducting the SHA are narrative; tabular; failure mode, effects, and criticality; fault hazard; fault tree; and plotting. Each method is briefly discussed in the paragraphs that follow.

6-2.2.1 Narrative and Tabular Analyses

These methods, usually associated with the PHA, present a discussion of a system, the hazards associated with that system, and the effects on the system and with corrective actions or safeguards. The analysis formats for these techniques are discussed in pars. 4-3.1.1 and 4-3.1.2.

6-2.2.2 Failure Mode, Effects, and Criticality Analysis (FMECA)

The FMECA, when used for preparing an SHA, should concentrate on component and subsystem failures leading toward system malfunctions. The FMECA is best suited for application to hardware for which failure modes and failure rates have been established. It analyzes hardware at the piece-part level and considers the interrelation as well as the relation to the whole system. The details of conducting an FMECA are presented in par. 5-3.

6-2.2.3 Fault Hazard Analysis

An FHA is a detailed investigation of the system to determine hazard modes, causes of these hazards, and the resultant effects on the operation of the system. Unlike the FMECA, the FHA considers human errors that could result from a particular hardware design. The details of conducting an FHA are presented in par. 5-4.

6-2.2.4 Fault Tree Analysis

The FTA is probably the most useful tool in performing an SHA. Fault trees can be developed for all of the major hazardous events that could happen when operating, testing, or maintaining a system. An FTA starting at the system level will show, in a logical manner, the affected interfaces among subsystems, components, personnel, and the operating environment. Critical sequences, timing, and single-point failures can also be noted in the fault tree. If the top event can be caused or initiated by a failure, a failure analysis must be undertaken. The details of conducting an FTA are presented in par. 5-5.

6-2.2.5 Plotting (Mapping) Hazards

Problems that could develop because of locations or proximities of units, lines, or hazards external to the basic system are frequently revealed by mapping. Plotting the problem graphically can illustrate existing potentially hazardous interrelationships. The examples that follow illustrate the types of situations for which this technique is appropriate. (See par. 4-3.2.3.2 for additional detail.)

1. Safety distances need to be established between fuel lines and ignition sources. The dangers are evident when fuel lines and engines are in close proximity. Leakage of fuel from a poor connection or ruptured line onto a hot surface could result in a fire. Many of these dangers can be identified from drawings that show the locations of fuel lines, connections, engines, spark-producing devices, and similar potential hazards. In such cases, the fuel lines should be designed with a minimum number of connections. The connections should be located where they cannot leak flammable fluid on hot spots or where a means of isolation separates the fuel line and the hot spot.

2. During the launch of a particular type of missile, the damper pads and end caps are ejected from the launch tube. The launch tube is then ejected from the launcher. Mapping would reveal the correct safety perimeter for personnel operating the launcher. Using the necessary test or dynamic analysis data, the safety analyst would construct two maps—one showing personnel locations and the other showing the trajectories of the ejected pads and caps and launcher tubes. He would overlay the two maps to assess the potential hazard and establish the possible need for some controls.

3. Locations of fuel tanks should be reviewed to

   a. Insure there is adequate separation between fuels and oxidizers so that leakage of either one will not result in contact with the other

   b. Determine the necessity for dikes or containment walls

SYSTEM/
MODEL _____
SUBSYSTEM _____

SYSTEM HAZARD ANALYSIS

ANALYST _____
REVIEW _____

PAGE ___ OF ___
DATE _____
DATE _____

IDENT.	A	B	C	D	E	F		G
	ITEM IDENTIFICATION AND INTERFACE	SYS. OPER. PHASE/ EVENT	HAZARD MODE OR EVENT	HAZARD EFFECT ON SUBSYSTEM/SYSTEM	UPSTREAM EVENTS THAT MAY INFLUENCE HAZARD	RISK ASSESSMENT		REMARKS, CORRECTIVE ACTIONS OR RECOMMENDATIONS -THEIR EFFECTS AND STATUS OF ACTIONS
ITEM NO.						HAZARD CATEGORY	HAZARD PROBABILITY	

Figure 6-1. System Hazard Analysis Tabular Form

c. Determine whether or not leakage could endanger personnel or facilities along channels through which the liquid would flow.

This type of mapping would also pinpoint possible hazards at a vehicle refueling depot.

4. Fig. 6-2 shows how mapping can be used to analyze the possibility of fires resulting from accidents involving Army helicopters. Although the mapping was used in an accident analysis of existing designs, it is undoubtedly an effective way to study whether or not similar hazards might exist in designs of new helicopters. The layouts will indicate the susceptibility of fuel tanks to rupture by landing gear after a hard impact and whether or not the proposed design of the landing gear should be reconsidered.

A study of helicopter crashes showed that 90% of the fires were generated at initial impact or immediately thereafter. In 80% of the fires, ruptured fuel cells and broken fuel lines caused spillage or leakage of fuel that ignited when it hit a hot surface, such as the exhaust system of the engine. In major accidents the helicopter generally rolls over and lies on its side, which blocks at least one of the personnel exits and limits the means of egress. In addition, the fuel tank might come to rest in a position to spill its remaining fuel onto the hot engine located below. Mapping will help to determine whether such problems might exist in new helicopters.

Therefore, before a human error analysis can be performed, the group defining the machine-to-human interfaces must develop a step-by-step description of the specific human operations to be studied. For the operations mode of a system, this group will consist of the designers and human factors engineers, who will be assisted by Army representatives from the using command. For the maintenance and support mode, the human interfaces will be defined by the maintainability and logistic personnel, together with human factors engineers, assisted by the designers and using command representatives. Once these definitions have been made, the safety engineers can study the human action steps to identify potential hazards in personnel error by considering the causes and contributing factors previously discussed.

6-2.2.6 Human Error Analysis

6-2.2.6.1 General

Human error can be defined as any personnel action that is inconsistent with behavioral patterns considered to be normal or any action that differs from prescribed procedures. Human error includes (Ref. 4)

1. Failing to perform a task (omission)
2. Incorrectly performing a task
3. Performing a task not required
4. Performing a task out of sequence
5. Failing to perform a task within the allocated time
6. Responding inadequately to a contingency.
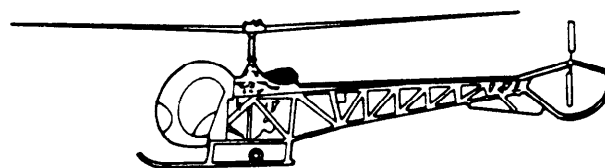
(A) OH-13 Models D and E Single Fuel Cell
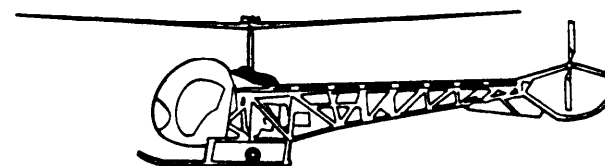
(B) OH-13 Models G and H Twin Fuel Cells (Both sides of rotor)
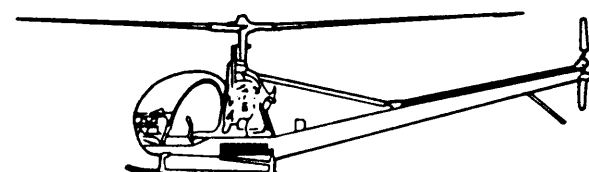
(C) OH-23 Single Bladder-Type Cell
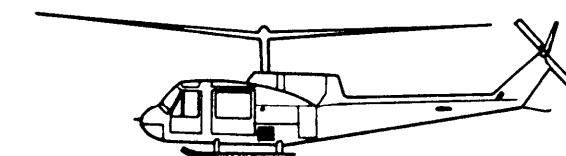
(D) UH-1 Bladder-Type Cells Aft and Outboard of Cockpit
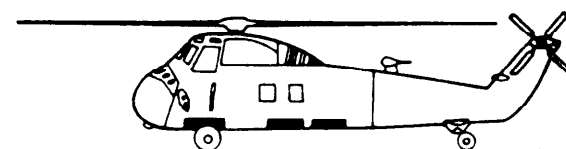
(E) CH-34 Three Fuel Cells
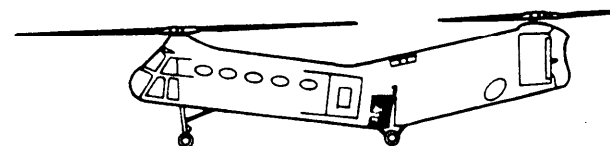
(F) CH-21 Fuel Cell Over Landing Gear
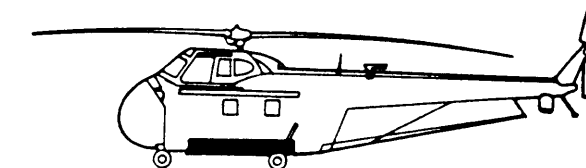
(G) UH-19 Fuel Cell Proximity to Landing Gear

Figure 6-2. Fuel Tank Vulnerability in Helicopters

Regardless of thorough training and high skill levels, a technician will make mistakes, and errors frequently cause equipment malfunction with varying consequences. For example, a driver fails to fill the radiator of a truck, the engine overheats, and the truck stops on the road—inconvenient but not serious. A technician fails to put a cotter pin in a castellated nut in the flight control linkage of an aircraft, control of the plane is lost in flight, the plane crashes, and all aboard are killed—very serious.

Maintenance requirements are so demanding that they often leave no room for human error, yet mistakes will be made. For example, a report by one of the military services revealed that in a 15-month period errors made in aircraft maintenance contributed to 475 accidents and incidents in flight and ground operations. Ninety-six aircraft were seriously damaged or destroyed, and 14 lives were lost (Ref. 5). A study of these accidents revealed that many of the failures that caused the accidents occurred shortly after periodic inspections. The report concluded that these human failures were caused by

1. Inadequate basic training in the relevant maintenance practices, policies, and procedures
2. Lack of training in maintenance of the types and modules of equipment being maintained
3. Inadequate or improper supervision
4. Inadequate inspection.

Knowledge about human error can reduce the probability of damaged equipment or personnel injury by imposing human factors constraints on the equipment design. The characteristics that follow contribute to human errors and diminish the safety of person/machine relationships (Ref. 6):

1. Population stereotypes, i.e., the manner in which most people in the population expect something to be done—e.g., when a control is turned counterclockwise, the controlled function is expected to increase
2. Performance requirements that exceed human capability
3. Designs that promote fatigue
4. Inadequate facilities or information
5. Unnecessarily difficult or unpleasant tasks
6. Necessarily dangerous tasks
7. Unpleasant tasks.

6-2.2.6.2 Quantification

A need exists to understand and predict the contribution of human error to the safety of a system from both an operational and maintenance point of view. In fact, some analyses reveal that the majority of system failures are attributable to human error and not to hardware. Accordingly, human error must be analyzed in combination with all of the other failure modes for the SHA.

Much work has been done in human performance reliability (HPR). Yet a basic problem remains, i.e., lack of a good data base of human error and performance (Ref. 7).

The models available are fairly sophisticated, but considering the poor quality of the data input to the models, the output should be used with caution. There are several HPR indices that differ both in scope and in type of model used. Two types—the technique for human error rate prediction (THERP) and the Siegel-Wolf model—will be discussed. Ref. 8 discusses other techniques.

The analytical or simulation THERP can be used to predict the total system or subsystem failure rate resulting from human errors (Ref. 9). The THERP methodology begins with a task analysis that divides the system into a series of personnel-equipment functional (PEF) units. The system being analyzed is then described by a functional flow diagram. Prediction data are assigned to each PEF unit. A computer program calculates the reliability of task accomplishment and performance completion time and takes into account dependent and redundant relationships.

The Siegel-Wolf digital simulation model is oriented toward the effects of time stress on the successful completion of the task. The model outputs are (Ref. 9)

1. Average time expended
2. Average peak stress
3. Average final stress
4. Probability of task success
5. Average waiting time
6. Sum of subtasks ignored
7. Sum of subtasks failed.

A good start on a data bank of human error rates has been made by the American Institute of Research (AIR) (Ref. 10). The AIR estimates of error rates are for average, trained military personnel with average motivation who are operating under normal conditions. However, very little work has been done to quantify the degradation of human performance under operational stress.

A second source of data results from an analysis of the maintenance data in The Army Maintenance Management System (TAMMS). Maintenance actions reported through TAMMS are analyzed and supplemented with independent judgments and arrive at quantitative values for human error data. Table 6-1 presents the results of a study that used this method. Human error rate estimates for a large system were derived from existing data of poor quality by modifying the data with the independent judgments of human reliability analysts (Ref. 10). These judgments were made after reviewing information on personnel skill levels; previous jobs held by these personnel; procedures; and design of the control, displays, and other equipment read or manipulated by the personnel.

To date, the primary source of HPR information is subjective data based on expert opinion or objective data supplemented as necessary with subjective judgments. Techniques for developing expert estimates include the Delphi Technique (Ref. 9).

The results of the human error analysis can be presented in the narrative, tabular, or even logic tree format

TABLE 6-1. HUMAN ERROR RATE ESTIMATE DATA (Ref. 10)

Estimated Rates	Activity
10^{-4}	Selection of a key-operated switch, rather than a nonkey switch. (The value does not include the error of decision where the operator misinterprets the situation and believes the key switch is the correct choice.)
10^{-3}	Selection of a switch (or pair of switches) dissimilar in shape or location to the desired switch (or pair of switches) assuming no decision error. For example, operator actuates a large-handled switch, rather than a small switch.
3×10^{-3}	General human error of commission, e.g., misreading label and thereby selecting wrong switch.
10^{-2}	General human error of omission where there is no display in the control room of the status of the item omitted, e.g., failure to return a manually operated test valve to proper configuration after maintenance.
3×10^{-3}	Errors of omission where the items being omitted are embedded in procedure, rather than at the end as in the previous activity.
3×10^{-2}	Simple arithmetic errors with self-checking but without repeating the calculation by redoing it on another piece of paper.
0.2-0.3	General error rate given very high stress levels where dangerous activities are occurring rapidly.

depending on how much information is to be provided about the human error and where it fits in the SHA.

6-3 SOURCES OF SYSTEM HAZARD ANALYSIS DATA

The major sources of generalized accident and reliability data are listed and described in Chapter 4, Appendix A. A review of field accident reports and hazard reports for fielded Army systems similar to the one under development will assist in performance of the SHA. More specific system hazard data will be found in documents pertaining to the system under development—i.e., system specifications, requirements document for mission parameters, and safety analyses (PHA, FHA, or FTA) that may have been performed earlier on the system.

The safety analyst should review the input requirements for each subsystem along with any possible safety-related restrictions or qualifications that may apply. Comparing input limitations of one subsystem with all possible outputs of an upstream subsystem will help in determining possible hazards and necessary safeguards.

6-4 EXAMPLE

The system hazard analysis shown in Fig. 6-3 was taken from an analysis performed on the Army Laser Target Designator. Two subsystems and their interface and hazards are shown in the figure. The analysis is represen-

tative, and only one page is included to show the format of the system hazard analysis.

6-5 ADVANTAGES

Each system-level safety analysis method can be used more advantageously in one circumstance than in another. The general criteria for determining which method would best serve for developing the SHA for a particular program are

1. How much data are available when the analysis must be made?

2. How much time is there to prepare the analysis?

3. How is the analysis to be used and for what purpose? (It is assumed that experienced safety engineers personnel will be performing the analysis.)

In the paragraphs that follow the advantages of the different analysis methods in relation to the circumstances will be discussed.

6-5.1 ADVANTAGES OF THE FAULT TREE ANALYSIS

The FTA has the advantage of depicting, in a diagrammatic manner, an adverse end event and the factors that could cause it. Thus an FTA quickly identifies the design areas—such as components or subsystems—that will require failure probability number values.

SYSTEM/
MODEL. Laser Target Designator
SUBSYSTEM _____

SYSTEM HAZARD ANALYSIS

ANALYST _____
REVIEW _____

PAGE ___ OF ___
DATE _____
DATE _____

IDENT.	A	B	C	D	E	F		G
	ITEM IDENTIFICATION AND INTERFACE	SYS. OPER. PHASE/ EVENT	HAZARD MODE OR EVENT	HAZARD EFFECT ON SUBSYSTEM/SYSTEM	UPSTREAM EVENTS THAT MAY INFLUENCE HAZARD	RISK ASSESSMENT		REMARKS, CORRECTIVE ACTIONS OR RECOMMENDATIONS THEIR EFFECTS AND STATUS OF ACTIONS
ITEM NO.						HAZARD CATEGORY	HAZARD PROBABILITY	
1	Battery	Operation	Rupture	1. Personnel injury 2. Damage to equipment	1. Direct short causing rapid discharge	I	C	1. Inspect battery connector to insure pins are not deformed or bent before installing. 2. Protect battery connector when not installed.
		Maintenance	Overheat	Damage to equipment	Overcharging during recharging	III	C	Monitor recharging operation to assure battery is not overcharged.
2	Transmitter	Maintenance	1. Pressure vessel rupture	1. Pressure vessel over-pressurization		I	D	1. Protect equipment from damage or misuse.
			2. Overheating	2. Damage to electronic circuitry	2. Failure of overtemperature sensing/interrupt circuitry	III	C	2. Insure preventive maintenance is performed by qualified personnel.
		Operation	1. Failure to cease lasing	Exposure of personnel to laser radiation	1. Trigger failure	II	B	1. Disconnect battery in event trigger, trigger circuit, or PFN circuit fail.
			2. Uncommanded lasing		2. PFN circuitry failure	II	B	2. Stop lasing in event surface temperature rises excessively.
					3. Trigger circuit failure			
			Electrical short	Fire from arcing	Insulation failure	II	B	Choose insulation that will withstand total environment and potting compounds that avoid polymerization over long periods.

Figure 6-3.   Example of an Army Laser Target Designator System Hazard Analysis

When the lowest levels of all branches of the fault tree have been assigned probability values, the probability numbers can be calculated for each succeeding higher level until the probability of the undesired event at the top is known. Not only does the technique allow determination of the risk, but review of the FTA diagram will show the contribution of different parts of the system to the total risk assessment. The FTA enables the analyst to determine the possible failures that will yield a given set of failure symptoms, and the critical paths and the safety impact of changes.

The FTA is also the best approach to use when specific undesired events are known to be possibilities in an alternative design under consideration. The FTA can provide management with information to assess the risk that these undesired events will occur if the particular design is chosen.

6-5.2 ADVANTAGES OF FAULT HAZARD ANALYSIS

The FHA in tabular format is more useful to show all the identified hazards in a design and provide information concerning each one. It is evident from an examination of the SHA shown in Fig. 6-3 that the hazard data are related to potential faults, their effects, causes, and corrective action. The SHA, using the FHA method, is at first a qualitative approach to a safety analysis that can be performed quickly and with only sketchy design data. Later, as detailed design data probability number values for failures become available, the tabular FHA can be updated as necessary. Thus it can provide useful inputs to other analyses. In the meantime, the FHA will be useful for comparing different alternative systems and presenting a general picture of the types and numbers of hazards in each alternative system.

The FHA method of developing an SHA can be particularly useful if a new system is to be developed by improving one already in the field. Then sufficient information will be available for preparation of an FHA showing qualitatively where safety will be affected by proposed changes for the new system.

For example, an existing personnel carrier may be a candidate for modification to incorporate an existing gun. An SHA could be prepared in a relatively short time to show qualitatively the hazards involved due to the interrelationships of each of these ex-systems, now subsystems of the new system. This SHA, in narrative form, could be developed from a previously prepared PHA to incorporate the additional detail concerning potential interface hazards, i.e., the effects on the transported personnel due to the firing of the gun. When specific, unwanted events have been identified in this manner, a decision can be made to prepare FTAs for quantification of those hazards. (This can only be done when sufficient data are available.)

6-5.3 ADVANTAGES OF FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS

The FMECA is more often prepared by the reliability engineers (Ref. 11). When data are made available by this technique to safety engineers, selected information from the FMECA can be used in a number of ways to evaluate the effects of failure modes on safety. The failure probabilities that have been assigned in the FMECA can be used for FTA or for special studies of safety-critical components.

Additional information of value to the program is also provided by the "criticality" section of the FMECA. This information includes

1. Identification of critical items that should be evaluated for the existence of hazards

2. Identification of items requiring special attention during production (such as special "high-reliability" parts) to insure no degradation in the safety level

3. Requirements for supplier specification data to insure that the designed-in safety level is maintained

4. Requirements for procedures, safeguards, protective equipment, monitoring devices, or warning devices

5. Where development funds can be applied most effectively to increase the safety level.

For example, an FMECA can identify a solid-state switch in a laser designator system which can either fail to operate or operate and fail (fail to close a circuit or fail in the closed circuit condition). The criticality analysis portion of the FMECA has identified the switch as safety critical because it can enable lasing to occur inadvertently when the system is turned on. The risk from inadvertent lasing can then be investigated for improvement—either by insuring that the switch is a very high-reliability item or by adding other circuits to prevent lasing unless the trigger is held down.

6-5.4 ADVANTAGES OF OTHER TECHNIQUES AND FORMATS

Advantages of techniques such as plotting or mapping become evident when the safety problem involves consideration of the geometry of space and dimension. Examples of problems involving the use of these techniques have been given in par. 6-2.2.5. When confronted with special circumstances in a particular safety problem, the safety engineer should use imagination, initiative, and logic to select one, or a combination, of the methods described or should modify them to suit the special circumstances.

New methods of safety analysis are being developed continuously by practicing safety professionals. These new methods are described in their periodicals and literature available at professional conferences. The new ideas should be considered for special circumstances.

6-6 LIMITATIONS

The initial SHA usually is accomplished before the system undergoes the first of the Materiel Acquisition Decision Process (MADP) reviews that may lead to design changes—i.e., in-process reviews (IPR), the Army System Acquisition Review Council (ASARC), or the Defense Acquisition Board (DAB). Accordingly, as the design matures, updates will be required to reflect the design changes and any new mission requirements or procedures that might affect system safety.

6-6.1 TIMELINESS OF SYSTEM HAZARD ANALYSIS INPUT SAFETY DATA

The SHA is limited in its scope by the level of detail to which the FMECA, FTA, and other analyses were performed. There are, however, two limitations in the use of the FMECA for safety. The first is that the FMECA will not be available at the time the SHA must initially be prepared, or, if it is available, it will be incomplete in the areas required for safety analysis. The second is that the completed FMECA will contain so much more reliability data than safety data that it will require lengthy study to identify the data useful to system safety. Much of the FMECA data relate to failures causing the system to fail to operate. This type of failure is generally a fail-safe mode, and most of the "failures to operate" are not of interest to safety engineers. These failures must still be reviewed because some of them—such as a vehicle engine failure—might constitute hazards. depending upon the system definitions.

6-6.2 SYSTEM OR SUBSYSTEM—BY DEFINITION

Any lack of information for defining system usage, location, environments (both natural and man-made), testing, maintaining, and storing will also place limits on the SHA. Other limits are placed on the analyst doing the SHA if the "system" is actually a "subsystem" of a larger, more complicated "system". For example, a missile system, when combined with a fire control system, might become a weapon system. This system, along with the launch platform, including other weapons, etc., could become an armament system. A clear definition of what constitutes a system and its total environment is essential to the SHA.

6-6.3 REQUIREMENT FOR PROBABILITY NUMBER VALUES

The FTA and any special safety studies that require probability number values for subsystems and components will also be limited by the lack of data, depending on program schedules. Although FTA logic diagrams and other analysis techniques can be drafted with whatever information is available, the reliability data that are the foundation for probability calculations are generally not available until considerable system and subsystem design work has been accomplished. Occasionally this limitation can be overcome if the particular analysis required has sufficient importance. In such a situation a priority can be established for a few specific reliability determinations in coordination with the ongoing design effort.

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.
2. Data Item Description DI-SAFT-80101, *System Safety Hazard Analysis Report*, 20 January 1986.
3. SAMSO STD 68-813, *Methodology for System Safety Analysis*, Space and Missile Systems Organization, August 1977.
4. W. Hammer, *Handbook of System and Product Safety*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1972.
5. AMCP 706-133. Engineering Design Handbook, *Maintainability Engineering Theory and Practice*, January 1976.
6. DH1-3. Design Handbook, *Human Factors Engineering*, Third Edition, Air Force Systems Command, Wright-Patterson AFB, OH, March 1977.
7. David Meister, *Subjective Data in Human Reliability Estimates. Reliability and Maintainability Conference*, 1978.
8. *Human Factors Review: 84*, Frederick A. Muckler, Ed., The Human Factors Society, Inc., Santa Monica, CA, 1984.
9. *Human Reliability Prediction System User's Manual*, Department of the Navy, Sea Command, December 1977.
10. A. D. Swain, *A Method for Performing a Human Factors Reliability Analysis*. Report SCR-685, Sandia Corporation, Albuquerque, NM, August 1963.
11. *SAE Design Analysis Procedure for Failure Mode, Effects. and Criticality Analysis (FMECA)*. SAE Aerospace Recommended Practice ARP926. 15 September 1967.

BIBLIOGRAPHY

DARCOM-P 385-23, *System Safety*, US Army Materiel Development and Readiness Command, Alexandria, VA, June 1977.

W. Hammer, *Product Safety Management and Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

R. A. Duregger, E. Leon, J. R. Sample, *System Safety Analysis Techniques as Applied to Shipboard Systems*, The Society of Naval Architects and Marine Engineers Meeting, May 1972.

AFSC DH-1-6, *System Safety*, Aeronautical Systems Division, Air Force Systems Command, April 1979.

CHAPTER 7
SOFTWARE ANALYSIS

The uniqueness of software—as compared to hardware—and how this uniqueness impacts system safety are discussed. Methods for insuring safe software are given. A concept for a method of analyzing software programs to determine whether program errors can generate, contribute to, or fail to control adverse safety effects in computer-controlled systems is presented. The application of the existing, conventional safety analysis techniques to software safety analysis is discussed. An example of a software safety analysis—based on a prototype air defense system—is provided. A software checklist is included to assist the analyst in performing a hazard analysis.

7-1 DESCRIPTION AND PURPOSE

Software safety analysis is the study of software programs to insure that the program—used in its intended operational environment—cannot cause or contribute to a hazardous condition. The need to consider the contribution of software to potential hazards was emphasized by the release of MIL-STD-882 (Ref. 1)—par. 4.3j addresses design requirements, and Task 212 requires the performance of a software hazard analysis. MIL-S-52779 outlines a quality assurance program for software (Ref. 2). The importance of computer software is highlighted by

1. The increased use of software to control hardware functions in weapon systems
2. The combat capability of weapon systems and the combat survivability of combatant units of the operating forces depend, in part, upon the effective operation of the weapon system software.
Accordingly, the traditional concept that the computer system—a "black box" that gives a specific output based on a given input together with its associated software—not be considered in a system safety analysis is no longer valid. Also the totality of software associated with a weapon system must be considered. Weapon system software comprises the software that is contained in the

1. Weapon system itself
2. Test and maintenance equipment
3. Training equipment
and includes the software used to develop, test, and support the weapon system software (Ref. 3).

Before delving into the system safety aspects of software, it is important to review some of the characteristics that make it unique, i.e., different from hardware. Software is a set of instructions, in a unique computer language, that tells a computer how to operate—i.e., what tasks and functions to perform. When the computer is incorporated into a system, the software communicates with the hardware elements by instructing them on when and what to do and on insuring that the tasks are performed. Thereby, a general-purpose computer can be used to accomplish anything from accounting to flying a spacecraft, depending solely upon the particular software program that resides inside the computer (Ref. 4). Distinguishing software characteristics follow:

1. Software is 100% reliable; it cannot fail; it may contain errors (faults), however.
2. Software is not subject to customary "wear and tear"; consequently, there are no failure rates as such.
3. Software will contain errors. Human programmers are not infallible—and because of the errors, the software may cause unexpected outputs that may be annoying, degrade efficiency and reliability, or generate a hazard.
4. Software does not break. It always works as designed but not necessarily as intended.
5. Software errors are built into the program, and the software usually does not stop functioning when an error occurs; the software merely continues to operate in an unanticipated manner.

An example of a mishap that occurred with a computer-controlled system is taken from Ref. 5:

"During boresight and zero training exercise, an M60A1E3 tank (with an old A7 XM21 Computer Card) fired a[n] [armor-piercing discarding sabot] APDS round with excessive super-elevation in the main gun. As the gunner was making a final lay on the target, the accumulator motor came on, the gun elevated; simultaneously the gunner fired. The ammunition indexed in the computer went from APDS to [high-explosive plastic] HEP. The gunner and tank commander were unable to initiate any corrective action to prevent the round from being fired. The round was observed impacting a greater range in the impact area.

"Commander, [US Army Test and Evaluation Command] TECOM, considers that the Tank, Combat, Full Tracked, 105-mm Gun, M60A1E3 does not meet all specified materiel performance requirements. Specifically, the XM21 Computer ammo reset was identified as a Category 1 safety deficiency...the [program manager] PM has determined that the problem is caused by low-voltage transients."

This definition of software will apply in the following paragraphs (Ref. 6):

"'Software' is defined as the totality of programs and routines used to extend the capabilities of computers such as compilers, assemblers, narrators, routines, and subroutines. This is contrasted with 'hardware', defined as

the mechanical, magnetic, electronic, and electrical devices from which a computer is fabricated; the assembly of material forming a computer.".

The software safety analysis to be discussed will deal with software, the signals loaded into the computer for processing by the software, and the output signals that result from the processing. The reasons for including inputs and outputs will be discussed later. In almost every instance, the scope of the software analysis must be restricted to make it a practical procedure. In addition, the method has been developed only for performing safety analyses of proposed or completed software programs; it is not intended as an instruction for writing programs or routines.

Problems in a software program can be identified in theory by testing the program to exhaustion in order to certify that it is correct and complete. The magnitude of that task, however, is illustrated by the following example (Ref. 7):

"...software certification is not easy. Ideally, it means checking all possible logical paths through a program; there may be a great many of these. For example,... [Fig. 7-1] shows a rather simple program flowchart....Even through this simple flowchart, the number of different paths is about 10^{20}. If one had a computer that could check out one path per nanosecond (10^{-9} second) and had started to check out the program at the beginning of the Christian era (1 A.D.), the job would be about half done at the present time."

Another writer (Ref. 8) states, "Probably the major weakness in all software testing methods is their inability to guarantee that a program has no errors. Exhaustive testing of even the most trivial programs is an impossible task, and the best one can hope for in a realistic testing effort is to find a high percentage of the remaining errors. This might lead to the question of whether there is some method other than testing that can be used to guarantee that a program is error-free...the answer is an emphatic no, and this answer is not likely to change in the future."

Such unfavorable prognoses require that a radically new approach be employed to achieve a usable method for software analysis. In effect, the method proposed here is as different from the usual lengthy, costly, and time-consuming method of testing computer software for safety purposes as fault tree analysis (FTA) is different from a failure mode, effects, and criticality analysis (FMECA). With both FMECA and the usual software

testing, *all* items in a product or program must be analyzed to achieve the end results. The determination of whether any unsafe conditions could occur is only one result of the total effort. With the FTA and the software analysis method proposed here, the analyst selects a safety problem and then identifies and studies only those factors that could contribute to the problem.

Two types of software safety analyses can be prepared using the proposed method, i.e.,

1. The first (initial) type of an analysis can generate data to alert designers and systems engineers to potential problems. Using these data, they can incorporate safeguards into the software programs and the input hardware to avoid the potential problems. The information can also be used for preparation of software and test specifications.

2. The second type of an analysis can insure that the completed software program contains suitable restraints to avoid erroneous inputs or the processing of such inputs and adequate provisions for preventing or minimizing undesirable outputs.

It is apparent that the problem of identifying and analyzing the causes of software hazards is not as obvious as the usual hardware safety problems a system safety engineer addresses. There is a uniqueness in the process of software analysis which requires the system safety engineer to attain a measure of expertise in software, firmware*, and computer architecture. Aware of this uniqueness, the safety analyst should be able to apply the conventional safety methods and techniques to the analysis of software systems with a reasonably high level of confidence to certify the safety of the product that the software controls.

7-2 HOW SOFTWARE IMPACTS SAFETY

As indicated in par. 7-1, although software does not have any failures *per se*, it does contain error mechanisms that can cause hazards. Research and experience have shown that the basic causes of software safety problems are (Ref. 3)

1. *Specification Error.* The software specification defines what, and sometimes how, the software is to perform. This is basically a description of the software/

---

*Firmware is a computer program, i.e., software that is implanted in hardware, e.g., as read-only memory.

Loop (≤12 times) Loop (≤12 times)
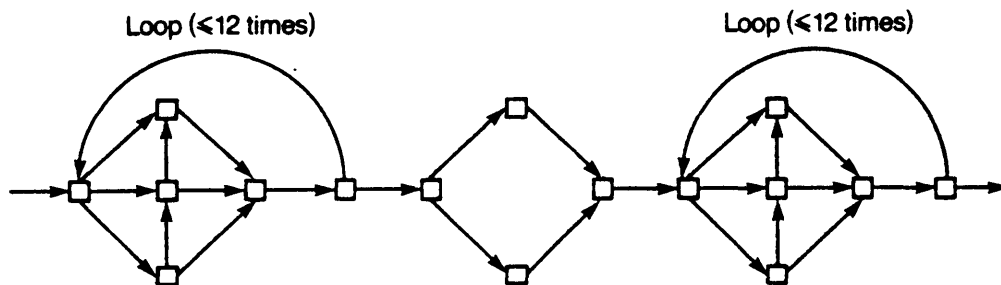
Figure 7-1. Simple Theoretical Flowchart (Ref. 7)

hardware interface. If a software/hardware interface is not properly planned, many unforeseen safety problems can result.

2. *Design Error*. In the software design phase, errors such as incorrect algorithms, incorrect interfaces, lack of self tests, etc., can result in safety problems.

3. *Coding Error*. In the software coding phase, errors such as incorrect signs, endless loops, unused logic, syntax errors, etc., are basically the problems that often are referred to as software "bugs". These errors generally result in reliability and quality problems, rather than safety problems.

4. *Hardware-Induced Error*. This is the hardware failure that results in the undesired transformation of a bit in a word. These bit errors change the entire meaning of a software instruction; sometimes the new meaning is acceptable to the computer, and sometimes it results in garbage that the computer will not accept. Hard failures—which are usually repeatable—can be traced and corrected; soft failures, however, occur randomly and usually are not repeatable when debugging.

The literature (Refs. 8 and 9) indicates that 60% of software errors are of the specification and design types. The studies, however, evaluated the overall software reliability and quality, and not strictly for the impact on system safety. In the judgment of the author of Ref. 4, most software safety problems stem from specification errors; accordingly, it is important that the safety engineer review the requirement document. It is the situation in which software/hardware interfaces are not completely understood and defined that safety problems arise because these cases cannot be foreseen in the specification. Also formal proof techniques only demonstrate the correctness of the software program with respect to the specifications, and there is no guarantee that the specifications are correct because the preparation of formal specifications is a difficult and error-prone process (Ref. 10). Not all software errors result in safety problems, and not all software that functions according to specifications is safe.

The generalized hazard categories can be classified as follows (Ref. 4):

1. *Inherent Hazard*. A software-controlled function that is inherently hazardous due to the hazardous nature of the equipment being controlled.

2. *Timing Hazard*. A software-controlled function in which the timing sequences are safety critical. This is often an overlooked area because sequences often are taken for granted to be safe until an accident occurs.

3. *Induced Hazard*. A software hazard caused by a computer hardware failure that causes a bit error; this results in an erroneous instruction. For example, an intended word "1101" meaning "add to Register A" may be changed by an induced bit error to "1011" that means "subtract from Register A".

4. *Latent Hazard*. A hidden condition in the software design that is not hazardous until a particular unplanned or untested set of circumstances occurs.

It is unnecessary that the safety engineer be an expert programmer; he should have suffcient knowledge, however, about the design of the software system to understand what functions or events are produced by which commands. It is also important to recognize that testing determines the presence of errors, not the absence. Software system safety is too important to be delegated to those who only understand programming.

7-3 METHODS FOR INSURING SAFE SOFTWARE

Software safety can be achieved by the application of engineering and management techniques during the software development process, i.e., (Ref. 4)

1. *Software Development Techniques*. These are special engineering techniques that are applied in the software development process during each phase of the software life cycle. For example, modular design and structured programming are used during the design and programming phase, and simulation can be used on the software as it is being developed to test how it performs in a simulated system environment.

2. *Software Management Techniques*. These are the typical management functions of planning, staffing, organizing, and directing which can be applied successfully to software. Some key elements are configuration control, proper scheduling, and up-to-date documentation.

3. *Safety Analysis Techniques*. These are the analysis techniques used by the system safety engineer to identify and control software-related hazards.

4. *Software Safety Standards*. These are safety standards and requirements which, if available, would be applicable to software modules as is currently done for hardware items.

5. *Standard Software Modules*. This is a concept similar to hardware part standardization whereby standard software modules could be developed and, when fully proven, could be applied to any project requiring the particular software function. The use of the ADA language by the Department of Defense can accelerate the process.

6. *Safety Configuration Control*. These are sections of the software code which are safety critical and should be so identified and controlled by the responsible organization. These particular sections of the code should never be modified without a special safety evaluation.

7-4 TECHNIQUE AND FORMAT

The technique and formats for the proposed method of software safety analysis were developed specifically to enable the analyst to identify safety-related software errors systematically by focusing on the firmware functions and the hardware/software interface. The technique and formats are described in the paragraphs that follow.

7-4.1 TECHNIQUE RATIONALE

A safety analysis of system software has the same general objective as all the safety analyses discussed in prior chapters, i.e., to evaluate a design—hardware and software—and to identify potential hazards existing in the system and the relative risks involved. In the software

analysis this objective translates into identifying software conditions that could inhibit desired functions or generate undesired functions. Until recently, the analysis of software programs was concerned with methods to detect *all* errors that might exist in a program. This goal was impractical—as pointed out in par. 7-1—because of the time required. Therefore, the original goal generally has been limited to analyses and tests of selected portions of the program. However, these may ignore potentially hazardous situations. To make the software analysis practical for safety purposes, the technique must be systematic and it must be limited. Also it must be organized to detect only those faults that could result in accidents caused by controller* outputs. Steps to perform a software analysis using this technique are

1. The analyst lists all the units of a system that would be affected by erroneous controller outputs. For each unit the analyst lists adverse safety effects that could result from software-related defects.

2. Next, the analyst selects the erroneous input signal to the unit that will create the adverse effect. This input signal to the unit will be an output signal from the controller. The aim is to minimize the generation of an erroneous signal and to control any such signal that might be generated.

3. The software program will be analyzed to determine

a. Whether any means exist whereby the erroneous output can be generated

b. Whether any means exist whereby the required safety-critical output can fail to be generated.

4. A determination will also be made whether or not the program incorporates means to eliminate or minimize the possibility that the erroneous output will occur.

5. The inputs to the controller will be analyzed to determine what inputs could cause an undesirable output (unless inhibited by a software routine). For example, an operating sequence might require that switches A and B be activated in that order. If only B is activated, or if B is activated before A, downstream units might be damaged or might initiate actions that could cause damage to other units. The software program, therefore, must contain provisions that will inhibit an output unless switch A is activated before B.

6. The analyst will then determine whether or not a source outside the controller, such as an operator error, can affect the program by modifying it or providing erroneous input data.

7-4.2 PROPOSED FORMAT

The proposed format for a software analysis in the tabular matrix format, consisting of Part 1 and Part 2, is shown in Tables 7-1 and 7-2, respectively. Part 1 (Table 7-1) is a report format compiling the results of the software safety analysis technique described in par. 7-4.1. This report is then evaluated to determine which line items are of sufficient safety importance to merit further

---

*The term "controller" includes the computer, input/output devices, a mass memory, and the rest of the hardware associated with the computer.

safety analysis. Part 2 (Table 7-2) is a more detailed software safety analysis.

Where necessary, the software analysis in tabular form can be accompanied with short narratives to provide detailed information too lengthy for inclusion in the table. For example, a system might have a controller with a number of units for inputs, processing, and performance. The narrative portion of the analysis might list descriptive features of each unit, such as processing characteristics or operating times, to insure that the features are all compatible.

The column headings used in Part 1 of the example format (Table 7-1) consist of descriptive phrases, to identify the type of information to be included in each column, as follows:

1. *Computer-Controlled Units of System.* All units that are directly computer controlled will be identified—whether considered subsystems, assemblies, or components.

2. *Adverse Events That Could be Initiated by Computer Output Error.* Each unit listed will be evaluated to identify every event it can be commanded to perform by either normal or abnormal output control signals from the computer. The consequences of the event will indicate whether it is—from a safety viewpoint—an adverse event or a normal, i.e., acceptable, event. For example, a simple "fails to operate" can be an unsafe event.

3. *Potential Effects of Adverse Event.* The adverse events for each unit are further defined as to all of their possible consequential effects on that unit and the other units with which it interfaces.

4. *Input Signal to Computer-Controlled Unit That Would Generate Each Adverse (Unsafe) Event.* Each adverse event is now analyzed to determine the type of input or lack of input that will cause it to function in the defined abnormal or unwanted manner. This signal or lack of signal is also the unwanted computer output signal or the signal that should be generated by the computer but is not produced.

5. *Proposed Safeguard.* The suggested change in the software or other types of change—hardware, warning device, procedure, or timing—that will prevent or reduce the probability of the unwanted event are described.

Part 2 of the software safety analysis is the detailed study. Column headings for Part 2 (Table 7-2) are defined as follows:

6. *Program Steps Which Could Produce or Permit the Unsafe Event.* The defective software logic point or lack of a software logic point that produces or permits the unsafe event is identified.

7. *Alternative Internal Program Actions Which Could Fail to Prevent the Unsafe Event.* Possible abnormal conditions existing with the unit that could receive the erroneous input are considered. The defective software logic or lack of logic to prevent the unwanted event in view of the abnormal condition is identified.

8. *Means of Avoiding the Alternative Action.* The logic change that will correct the condition described in Column 7 is identified.

9. *Control to Limit Alternative Action Which Can-*

TABLE 7-1. DETAILED INFORMATION ON SOFTWARE ANALYSIS (PART 1)

System _____

1 Computer- Controlled Units of System	2 Adverse Event That Could Be Initiated by Computer Output Error	3 Potential Effects of Adverse Event	4 Input Signal to Computer- Controlled Unit That Would Generate Each Adverse (Unsafe) Event	5 Proposed Safeguard

not be Eliminated. A possible software change that can affect intermediate conditions between those presented in Columns 7 and 8 is described.

10. *Means of Identifying Erroneous Output.* The software or combination of software and hardware changes that will go beyond simply preventing the unwanted event as indicated in Columns 8 and 9 is described, and the erroneous output or lack of output signal from the controller is now identified.

11. *Means of Inhibiting Erroneous Output.* Descriptions in the other columns deal with means to prevent the unwanted event due to an erroneous output and to identify the erroneous output. The software changes that will inhibit the erroneous output are described here.

12. *Inputs to Controller That Can Cause Unsafe Output Signal(s).* Conditions that could cause the erroneous output signals are described.

13. *Program Step to Avoid or Identify Erroneous*

Input. Software subroutines or other techniques that will determine that erroneous signals are being inputted into the controller are described. Possible corrections to prevent generation of erroneous signals are indicated.

14. *Program Step to Inhibit Processing Erroneous Input.* The software program step that will refuse to process an erroneous signal or that will inhibit outputting an erroneous signal is described.

15. *Operator Capability to Change Program, or Words, or to Provide Erroneous Inputs.* Interfaces, if any, that exist between the operator and the software are described. Can the operator bypass the output logic of the software in any manner?

16. *Remarks.* Any software, hardware, procedure, or management actions which affect the outcome of the events described are detailed.

In addition to the column headings shown in Tables 7-1 and 7-2, the analyst may find it desirable to include

TABLE 7-2. DETAILED INFORMATION ON SOFTWARE ANALYSIS (PART 2)

6	7	8	9	10	11
Program Steps Which Could Produce or Permit the Unsafe Event	Alternative Internal Program Actions Which Could Adversely Affect This Step	Means of Avoiding Alternative Action	Control to Limit Alternate Action Which Cannot Be Eliminated	Means of Identifying Erroneous Output	Means of Inhibiting Erroneous Output

columns that contain

1. Recommendations for specific tests to verify the adequacy of the program. This will inform software test personnel that a test is required for safety purposes.

2. Information on controller hardware interfaces that affect the software program. It may be possible that a hardware deficiency—such as transient voltage changes because of poor regulation—can wipe out computer programs, addresses, or information. This evaluation can be performed by using "clues" similar to the methodology for sneak circuit analysis (SCA) (See par. 5-6.) and software sneak analysis (SSA).

3. Information on common failure mode causes and effects. The failure of a software program routine could cause multiple effects whose interrelations should be described if safety related.

4. Processing times when their durations or intervals are safety critical—e.g., controller time to process a safety-related routine—could affect weapon firing or the interruption of firing.

5. Recommendations for requirements to be included in computer program development specifications.

6. Critical values should be indicated. Ref. 11 states the following on page B-17: "Many elements that have a range of values will have one value that is particularly significant to the analyst. This may be a breakpoint, a minimum stock level, a critical wind velocity, etc. When applicable, the critical value and its significance to the analyst should be included."

7. Check words and check values that should be used by the controller to recognize input, computer, or ouput errors (Ref. 12). This will avoid unexpected inputs that have caused computer-controlled incidents—such as 105 V, interpreted as 5 V—by insuring that values of received signals are within stipulated values.

TABLE 7-2. (cont'd)

12 Inputs to Controller That Can Cause Unsafe Output Signal(s)	13 Program Step to Avoid or Identify Erroneous Input	14 Program Step to Inhibit Processing Erroneous Input	15 Operator's Capability to Change Program, or Words, or to Provide Erroneous Inputs	16 Remarks

7-5 ANALYSIS TECHNIQUES

Because of the newness of the concept and techniques of software system safety analysis, hard data, e.g., error rate, are not yet available to provide "numbers" to augment existing system safety analysis methods. Eventually, however, error rates in software may become available when sufficient software test result data have been accumulated. Just as for hardware systems, the following existing system safety analysis methods are applicable:

1. Preliminary hazard analysis (PHA)/fault hazard analysis (FHA)
2. Logic diagrams
3. Fault tree analysis (FTA)
4. Nuclear safety cross-check analysis (NSCCA)
5. Software sneak analysis (SSA)
6. Operating hazard analysis (OHA).

"A good understanding of the design methods employed in the creation of the software system is very helpful, if not essential, in conducting the safety analysis. If the software designer used the structured top-down approach, then the same approach should be used by the system safety engineer in performing the analysis. This is why it is important for the safety engineer to be involved in the software system from the beginning of its life cycle. When a software-induced hazard is identified, the undesired event caused by the hazard can be declared as the top event. The top-down approach of the software safety analysis will lead to the cause of the hazard. Once the cause is determined by the safety engineer, the hazard controls can then be recommended and applied by the software designer.

"In performing the analysis, the safety engineer must also include firmware functions and the software/hardware interface. This interface can be easily understood if the safety engineer can identify the hardware event that will be driven by a software action. Usually, safety problems surface in software when these interfaces are not well defined by the software system designers. Lack of adequate interface definition results in specification errors, many of which produce hazards or undesired events. This

is another reason for safety engineers to be involved from the beginning of the system life cycle. They should participate in every walk-through and design review of the system. The more software errors that can be detected early in the life cycle, the more potential hazards can be eliminated by design changes.

"Every software module is designed to accept known inputs and produce known outputs. Errors produce unknown, and probably undesired, output which can, in turn, produce the undesired event. In many situations, errors exist in tested and accepted software and can go undetected for as long as the path containing it is not used. Such an error can be the one which will cause the undesired event." (Ref. 13)

The listed techniques work extremely well with hardware systems; however, they may not be equally applicable to software systems. The applicability of these techniques to software is discussed in the paragraphs that follow. Note that the familiar failure mode and effects analysis (FMEA) has been omitted. Since there are no components in software and there are no pure failures, an FMEA is not really useful and its application may be a waste of time and resources. The results of these analyses provide the bases for the detailed software analysis indicated by Tables 7-1 and 7-2.

7-5.1 PRELIMINARY HAZARD ANALYSIS/FAULT HAZARD ANALYSIS

"One of the most important system safety analyses is the Preliminary Hazard Analysis (PHA). In purely hardware systems, the PHA is used to identify as many hazards as possible early in the system life cycle. When applied to software/firmware safety analysis, the PHA may be in the form of Fault Hazard Analysis (FHA). The FHA becomes a more useful preliminary analysis method since the system safety engineer will be concerned with identifying hazards which are caused mostly by software errors. Determining these errors early in software life cycle will reduce the amount of rework which has to be performed because the corrective action can be implemented in the design as soon as the hazard-causing fault is determined. The FHA should precede other software safety analyses that may be performed. A well-compiled software safety checklist should be used in performing the FHA." (Ref. 13). A sample software safety checklist is shown in Table 7-3.

TABLE 7-3. SOFTWARE SAFETY CHECKLIST (Ref. 13)

1. Are logic decisions made in software verified by special logic built into each module?

2. Does software logic verify the sequence and logic of all keyboard actions?

3. Are routines that compute and/or set critical signals distributed over as many short sequence paths as possible?

4. Is control returned to the local executive as soon as is practical after the completion of a critical signal routine?

5. Is there more than one critical signal state processed in any of the critical signal paths?

6. Are internal software representations of functional discretes regularly updated and are flags represented by multibit patterns or bytes?

7. Do critical program routines use primary command inputs for logic and computation?

8. Are input data erased after each reading? Does software test the data buffer for presence of new data at the time of the next reading?

9. Does the software include a comprehensive self-test program which will be activated frequently when the system program is in operation? Does this self-test program have the capability of detecting all discrepancies in global data caused by interference from other software, read-only-protection error, and effects of inadvertent or malicious program alterations?

10. Are adequate provisions made for system backup or redundancy?

11. Are alarms used to alert to inadvertent or unauthorized software actions?

12. Are protocols and data extraction techniques for communication between data systems explicitly stated?

13. Are procedures described that assure the prompt detection and correction of deficiencies which otherwise could result in noncompliant software?

14. Are provisions made for a transition to degraded or manual mode if hardware failure or software error occurs?

7-5.2 LOGIC DIAGRAMS (Ref. 13)

"A logic diagram is a pictorial representation of the path software takes when a state and condition are known. A simple logic diagram can represent a single program instruction such as the one shown in...[Fig. 7-2]. Complex logic diagrams are constructed from simpler ones.

"Logic diagrams are of different types and can be used for different purposes. As an aid in software design, data flow diagrams are used, and there are a variety of these diagrams. Example of a data flow diagram is shown in... [Fig. 7-3]. Operational sequence diagrams are used in analyzing operations and time lines. State diagrams are used in software development to indicate control flow and to define process and process termination states....[Fig. 7-4] is one example of a control flow diagram. Certain data flow and control flow diagrams can be developed down to the level at which programmers can code directly from the diagram.

"Logic diagrams, when used in software safety, will probably produce another form of flow diagram. These diagrams describe the logic flow of data in software systems, modules or parts of modules. The use of logic diagrams then would be a description of data flow in the design-intended manner or nondesign-intended. Basically these diagrams are better understood and useful if the major levels in the diagram are also understood.

"In applying logic diagrams to software safety, each diagram must contain levels showing the undesired events, then the contributing events, and the error or failure that could cause the contributing events. The contributing event can be the wrong output of a module, and

Figure 7-4. Control Flow Diagram (Ref. 13)
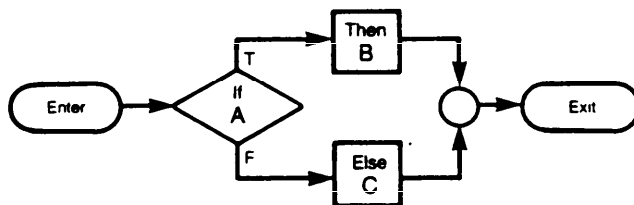
Figure 7-2. Software Instruction Logic Diagram (Ref. 13)
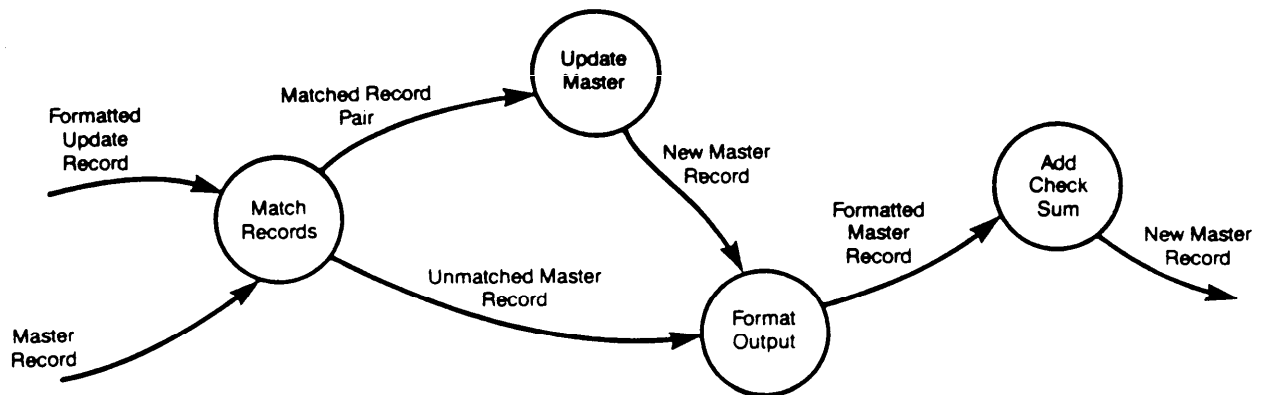
Figure 7-3. Data Flow Diagram (Ref. 13)

the cause of the contributing event could be a hardware failure or firmware error.

"All the diagrams mentioned above are not enough to demonstrate that process terminations of the software system processes are acceptably safe (free of error) or that the risk of hazardous process terminations is acceptably low. For the purposes of software safety analysis, logic diagrams, known as binary trees, should be constructed. Examples of these diagrams are shown in...[Figs. 7-5 and 7-6]. These binary trees should reflect a one-to-one correspondence between nodal branch points of the tree and the software decision points. They should also reflect that each branch can be categorized into a series of states and separated by state transitions, such as predicate transforms and algorithms, and which in turn can be described by Boolean expressions. The origin or the input to each tree should always be an operation, an interrupt, or return to higher level process. The ends of tree branches are process terminations or holds for operation responses.

"A Binary State Transition Tree, as in...[Fig. 7-5], is constructed to represent the normal operation of a software system at all process levels which are safety critical. The system safety engineer performing the analysis will use the tree to determine if system errors exist, and which are caused by program errors or by single or multiple hardware failures. System errors may be treated as a virtual branch in which the occurrence and subsequent processing can also be treated as a binary tree.

"A Binary Fault Termination Tree, as in...[Fig. 7-6], is of primary consideration in the software safety analysis because the ends of this tree may define hazardous termi-

nations. These trees are essential in analyzing whether checkpoints and procedures have been established to trap and contain software errors. This implies that there must be points which ascertain that a process has been legally entered, that the predicate transform or state vector is correct, and that data and messages have been verified before and after processing. When errors leading to hazardous termination have been identified, then a statistical method can be employed to compute the probability of a hazardous termination. The computed probabilities for hazardous terminations can be used in evaluating the risk for inadvertent processing of critical functions which were not contained by traps. Computed probabilities may be used to determine the necessity for modifying the software in order to reduce or eliminate the probability of an undesired event."

Fig. 7-7 contains the transition tree symbol legends associated with Figs. 7-2 through 7-6.

7-5.3 SOFTWARE FAULT TREE ANALYSIS (Ref. 13)

"Fault tree analysis (FTA), another form of logic diagram, has proven very useful in the analysis of hardware systems. It can be just as useful in the analysis of software systems especially when the analysis includes the software/hardware interface. The FTA uses the same basic methodology as the binary tree discussed in the previous section [par. 7-5.2].

"Software fault tree, or soft tree as it is sometimes called, involves identifying the logical paths leading to a top undesired event or process termination. Like the
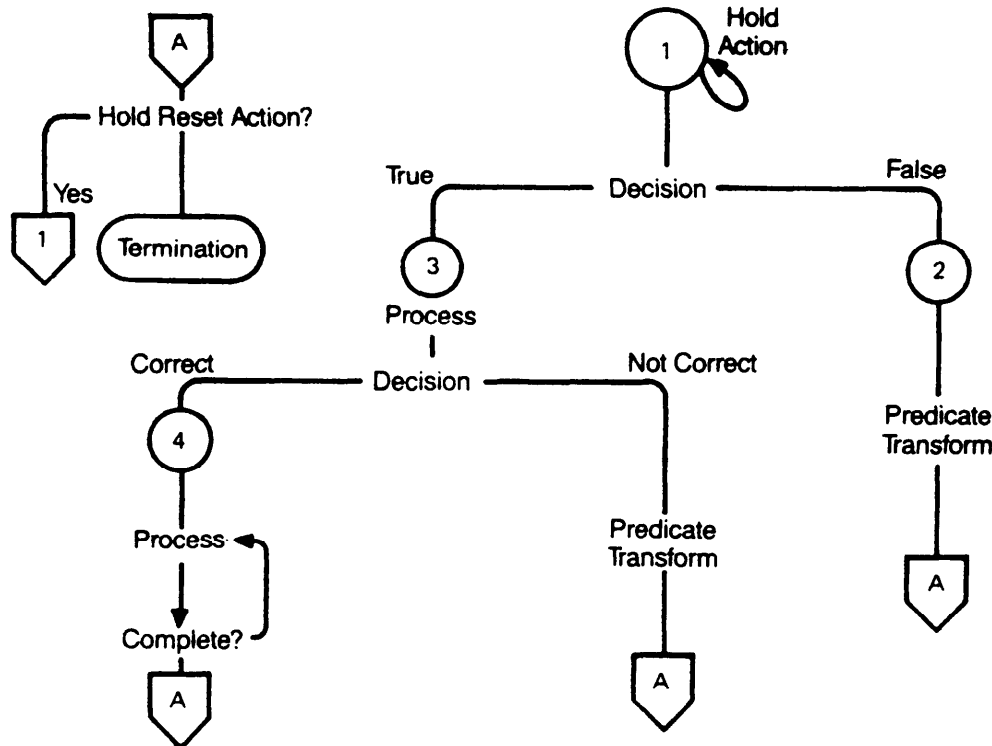
Figure 7-5. Binary State Transition Tree (Ref. 13)
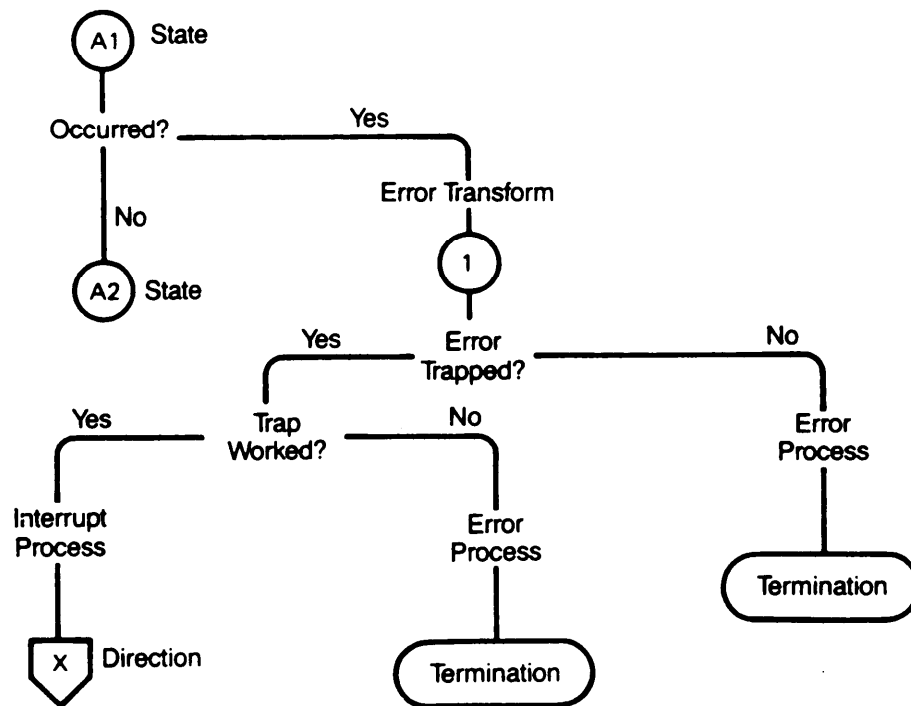
Figure 7-6. Binary Fault Termination Tree (Ref. 13)
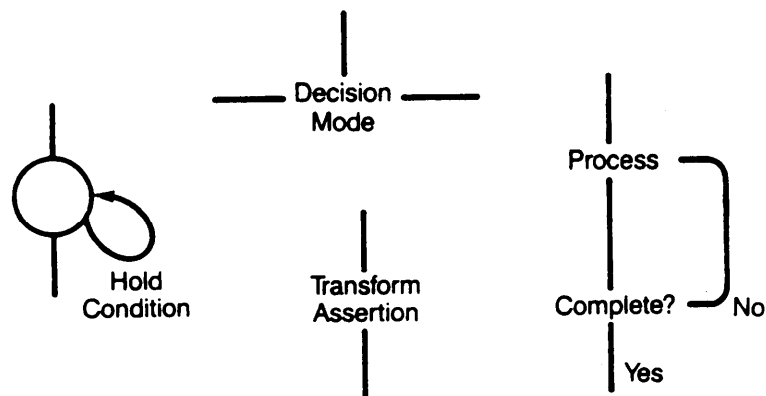
Figure 7-7. Transition Tree Symbol Legend (Ref. 13)

FTA, soft tree uses a deductive approach to identifying these critical paths, both qualitatively and quantitatively, and provides the minimal sets of states or critical paths which will lead to the top event. These minimal cut sets are important in the soft tree because they provide the unique path for the occurrence of the top event. Many useful techniques have been developed to find these critical paths such as Boolean reduction, deterministic testing, and simulation. Quantitative methods can be used to determine the likelihood or probability of the top event occurring using the numerical ranking by importance of individual faults.

"In soft tree analysis, however, the quantitative approach is not easily determined because there are no failures or failure rates in software. The quantitative methods in soft tree analysis are nevertheless possible if error or fault rates are used in place of failure rates. Error rates in software can be achieved if sufficient software test results data can be accumulated.

"Since the ultimate purpose of the soft tree analysis is to

achieve total system safety, then it is important to include the total system in the analysis. By this I mean all the elements of automata* including software/hardware interfaces should be included in the analysis. The usefulness of soft tree analysis is determined by the timing of the analysis itself. For this reason it is essential that the system safety engineer begin with preliminary and fault hazard analyses early in the system life cycle, and then implement the soft tree analysis. The soft tree analysis should be used at various levels and phases of the software system. With this approach safety can be designed into the system during its development.

"The previous two sections [pars. 7-5.2 and 7-5.3] described the logic diagrams and soft tree analysis methods which are useful in performing software safety analysis. The application is unique in that a model of the software system is diagrammed to reveal possible abnormal behavior. These analysis techniques will identify paths in the software system which are critical. They may also identify unused paths and paths which may lead to hazardous terminations. The logic of the soft tree approach makes it a tool to increase visibility for both engineering and management."

7-5.4 NUCLEAR SAFETY CROSS-CHECK ANALYSIS (Ref. 13)

"Nuclear Safety Cross-Check Analysis (NSCCA) is used in analyzing systems which command and control nuclear functions. It was developed specifically to satisfy requirements of Air Force regulations. The purpose of it is not simply to perform a safety analysis on the software, but also to show with a high degree of confidence, that the software system will not cause the initiation of undesired events. Therefore this type of analysis includes hardware as well as hardware/software interfaces. NSCCA is performed in two segments. The technical segment of this analysis determines if the software and the total automata system, by evaluation and test, satisfies the specified nuclear safety objectives. The technical segment utilizes a criticality analysis (CA). The procedural segment implements required security and control measures.

"The CA usually complements other analyses by extending the results of the other analyses and categorizing the criticality of hardware failure modes previously identified according to their expected frequency of occurrence and their effect on system performance. CA is a procedure which relates the probability of a hardware system component failure, or a software system module errors to a defined critical event such as loss of life or inability to perform a required function. The CA combines the severity level and hardware failure or software error rate to establish a risk or seriousness of the effects. The severity level values and their corresponding probabilities are used in the construction of a matrix indicating

the distribution of criticality. The relationship permits a criticality threshold to be established in order to identify 'critical' situations. Corrective action priorities can then be made from the list of critical items obtained from the matrix.

"A CA can be performed using either a qualitative or quantitative approach. The selection of the approach to be used depends on the availability of data from operational experience and tests which have been performed on similar systems under similar usage. If realistic data cannot be obtained, then the qualitative CA approach should be followed. In the qualitative approach relative probability and severity levels are used. The combination of the two levels establishes the relative criticality of the considered event.

"In the NSCCA the CA is an evaluation of the nuclear safety objectives by assessing them against the discrete software functions. A qualitative assessment is made as to the degree to which each software function impacts the nuclear safety objectives. Recommendations and suggestions are then made for how best to measure the software functions."

7-5.5 SOFTWARE SNEAK ANALYSIS (Ref. 13)

"Another analysis tool which has been used successfully in software/hardware integrated systems is the Software Sneak Analysis (SSA). [See par. 5-6.] Derived from the sneak circuit analysis technique used to analyze electrical/electronic circuitry, the SSA is used to identify software sneak paths. These are logic control paths which can cause an unwanted operation to occur or which bypass a desired operation without regard to failures of the hardware system to respond as programmed. When this condition occurs in circuits, paths, or software branches, a hazard, referred to as latent hazard, may exist.

"The purpose of SSA is to detect and identify these latent or 'sneak' conditions which can cause an undesired and unplanned function or process to occur. SSA provides an effective method for verifying all paths in software and those paths interfacing with hardware. Software and hardware designs are becoming more complex and the integration problem becomes more difficult. SSA has proven to be very effective in the area of verification of software/hardware interfaces and their proper functions in very complex systems.

"Performing SSA on software systems will increase confidence in system safety, will result in program cost savings, and will reduce delays in system development. The extent of applying SSA to software is determined by the results of fault-tree and soft-tree analyses. The network trees produced will provide the data required for other detailed analyses. Sample of a network tree is found in...[Fig. 7-8]. These network trees are also used as a design change control tool during the design phase of the system. Software sneak analysis is effectively applicable to software systems, and it has become such an important tool that it is already included in many military specifications.

---

*Automata is the assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention.
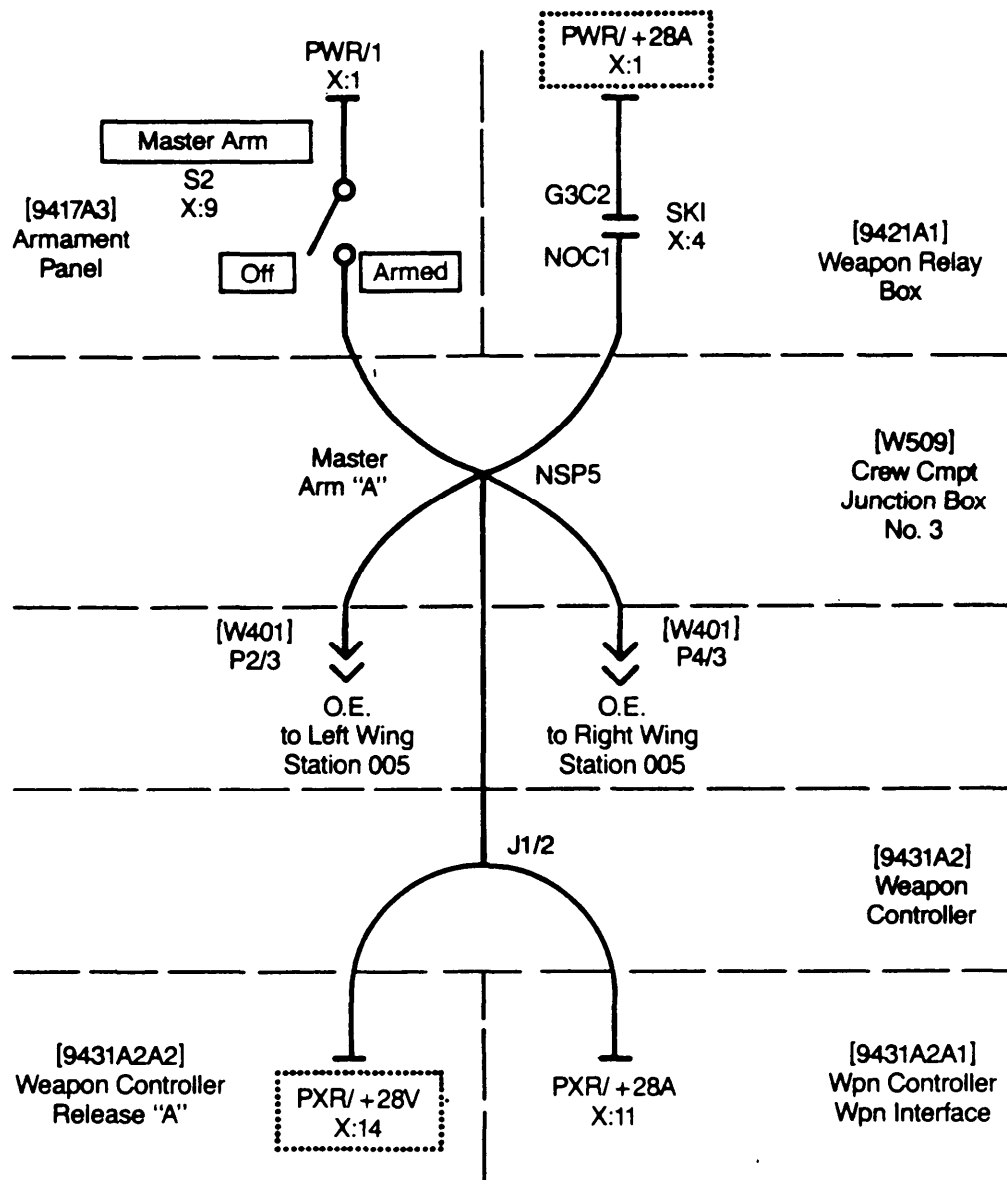
Figure 7-8. Topographic Network Tree (Ref. 13)

"SSA can be considered a mini- or microsoft tree; since it is simply a detailed analysis to the component level, of a node, a branch in a sublevel of a soft tree. Since SSA contributes to other detailed safety analyses of critical components or subsystems, it is always desirable to conduct this type analysis in the critical areas (within budgetary limitations). The analysis itself is so detailed and time-consuming that, like FTA, computer programs have been developed and are used effectively to chart the topological network trees."

It is important to point out that an SCA of software will locate many of the coding and design errors in a program, some of which may be hazardous; however, an SCA will not overly identify hazards (Ref. 4).

7-5.6 OPERATING HAZARD ANALYSIS (Ref. 13)

"In considering the applicability of Operating Hazard Analysis (OHA) to software safety, it is important to first understand the purpose of the analysis in general. The OHA provides the basis for inputs to detail test operation and maintenance plans and procedure reviews. The development of safety sequence charts and sequential task flow block diagrams is essential for the analysis to identify the tasks which require mandatory sequencing and those which can be concurrent. The total system must be interactively evaluated.

"For any analysis on software, to be meaningful, it has

to be evaluated in the operating mode. The basic functional definition of software asserts that it is in operation by stating that software is the automated execution of sequential task instructions used in controlling the operation of computer hardware.

"Various methods may be used to supplement the OHA such as desk checking. This method manually simulates program execution in order to understand and verify program logic and data flow. At times desk checking should be used to supplement the safety analysis being performed. The benefit of doing this is that some areas of the software can be more cost effectively evaluated by the method of desk checking.

"As the name implies, a software OHA is used to identify software operating hazards. We know that a hazard is any condition, existing or potential, which could conceivably cause an accident resulting in loss, but the concept of an accident occurring in software alone does not exist. Thus when we refer to software hazards in system safety, it should imply the hazards associated with the whole system of software, the hardware with which it interfaces, and the operating personnel. Thus the software OHA is not a software only analysis, but should include in context, the whole automata system and all the other hardware systems controlled by it."

7-6 EXAMPLE

The software safety analysis technique discussed in this chapter has never been rigorously applied but was developed for a specific application. Most of the information used in Tables 7-4 and 7-5 and in Fig. 7-9 was derived from the design of that prototype system but has been modified to indicate how the proposed technique would be applied to the XW-91 Army Air Defense System (a hypothetical computer-controlled weapon system).

7-6.1 BACKGROUND

The XW-91 consists of a vehicle-mounted automatic weapon intended to destroy incoming enemy missiles and aircraft. The weapon is located in a turret that provides protection for both the operating crew and the weapon itself. The turret and the weapon are moved hydraulically, the turret in azimuth and the weapon in elevation. Movements of the turret and its window are limited—by computer control, by hardstops, and by electromechanical limit switches—so that the weapon will not fire into the vehicle where it is mounted, nor into the ground nearby.

The computer control has been programmed to inhibit firing into any proscribed areas by means of data identifying the boundaries of those areas. Before the weapon can be fired, a cover must be moved out of the way. The movement of the cover is controlled by the software program, and the program has been designed to leave the cover in place until just prior to firing.

The radar picks up and tracks the target missile or aircraft and provides slant range information to the controller. Azimuth and elevation data from resolvers on the turret and weapon mount are fed to the controller. The

controller will determine angle and distance to the target, and it will permit firing when all necessary conditions in its software program are satisfied. If at least one condition is not satisfied, firing will be aborted. For this example, the abort system has been selected to demonstrate the proposed technique of making a software analysis.

7-6.2 LOGIC

The conditions that must be satisfied to fire the XW-91 weapon, listed in terminology familiar to any design engineer conversant with methods of logic, follow:

PA = weapon pointing to a safe area

$\overline{PA}$ = weapon not pointing to a safe area

(Note: The bar over a symbol will indicate "not" in accordance with accepted logic notation.)
and

$$PA = PZ \char"005E PE \qquad (7\text{-}1)$$

(See par. 5-4.1.4 for Boolean algebra symbols and rules.)
where

PZ = satisfactory azimuth position

PE = satisfactory elevation position.

To determine these conditions, the software logic checks

TT = weapon on target

HS = hydraulic system operating properly

PS = power system operating properly

CS = computer system operating properly

CFO = protective cover fully open

CC = protective cover closed

TD = target within range.

An abort consists of either one or both of the following actions:

1. *Inhibit.* To prevent initiation of an action
2. *Interrupt.* To stop an action in progress.

Use of the word abort means that both inhibit and interrupt would occur. (In some cases, separate analyses for inhibit and interrupt may be required.) An abort in this system will occur if any of the previously indicated conditions fail to meet the limitations imposed in the software. When a positive condition is required, any failure that causes the absence of that positive condition will result in an abort. The Boolean expression that indicates the relationship for aborts in terms of the governing conditions is

$$Abort = \overline{PA} + \overline{CFO} + CC + \overline{TT}$$
$$+ \overline{TD} + \overline{HS} + \overline{PS} + \overline{CS}. \qquad (7\text{-}2)$$

7-6.3 COMPUTER SOFTWARE PROGRAM

The computer software program routine for the abort process is shown in Fig. 7-9. This routine is a limited portion of the entire software program. Further, the example shown in the analysis technique will use only one item, XW-91-700, of this routine. Tables 7-4 and 7-5 will indicate how and why this item was selected and will start with a review of computer-controlled subsystems. Certain

TABLE 7-4. DETAILED INFORMATION ON SOFTWARE ANALYSIS (PART 1) FOR XW-91 SYSTEM

System: XW-91 Army Air Defense System

1 Computer- Controlled Units of System	2 Adverse Event That Could Be Initiated by Computer Output Error	3 Potential Effects of Adverse Event	4 Input Signal to Computer- Controlled Unit That Would Generate Each Adverse (Unsafe) Event	5 Proposed Safeguard
1. Turret				
2. Weapon	2a. Weapon fires inadvertently.	2a. (1) Hit on unintended target. (2) Hit protective cover which is not fully open. (3) Waste of ammunition.	2a. Failure to inhibit weapon firing signal.	2a. (1) Software program to inhibit firing unless all safety conditions are satisfied. (2) Software program to inhibit firing unless protective cover is fully open. (3) Not a safety problem.
	2b. Weapon fires into proscribed area.	2b. (1) Damage to own vehicle. (2) Injury or damage to nearby personnel or equipment.	2b. Failure to interrupt weapon firing signal.	2b. (1) Software program will interrupt firing if a command would direct the weapon into the proscribed area or if line of sight of the weapon approaches the limit to that area. Also, mechanical stops to prevent firing into proscribed areas. (2) Same.

TABLE 7-5. DETAILED INFORMATION ON SOFTWARE ANALYSIS (PART 2) FOR XW-91 SYSTEM

System: XW-91 Army Air Defense System

Short Description of Hazard Being Analyzed: Possibility that controller will permit weapon to be fired when protective cover is closed.

6	7	8	9	10	11
Progress Steps Which Could Produce or Permit the Unsafe Event	Alternative Internal Program Actions Which Could Adversely Affect This Step	Means of Avoiding Alternative Action	Control to Limit Alternate Action Which Cannot be Eliminated	Means of Identifying Erroneous Output	Means of Inhibiting Erroneous Output
2a(2). Current program permits weapon to fire only when "Cover Fully Open" signal is received, even if cover is actually closed. Noise or electro-magnetic effect could erase a critical instruction.	2a(2). Failure in software program to include provision to inhibit firing when a short circuit results in "Cover Fully Open" and "Cover Closed" signals are both inputted to controller. (Controller acts only on "Open" signal.)	2a(2). Modify software program so that firing will be inhibited unless both "Cover Fully Open" AND no "Cover Closed". Check subroutines to insure they will satisfy all foreseeable requirements and inputs.	2a(2). Only remaining possibility not covered by software program is that cover might be partially open AND there might be an erroneous "Cover Fully Open" input signal. Probability of these occurring simultaneously is so remote it can be disregarded.	2a(2). Provide an additional input signal (photoelectric cell or interlock at cover) and comparison routine in software programs.	2a(2). Provide redundant routines and compare after completion. If they do not correspond, inhibit firing. Repeat routine three times (TMTI-Tell Me Three Times) to insure it is not a one-time processing error.

TABLE 7-5. (cont'd)

| 12	13	14	15	16
Inputs to Controller That Can Cause Unsafe Output Signal(s)	Program Step to Avoid or Identify Erroneous Input	Program Step to Inhibit Processing Erroneous Input	Operator's Capability to Change Program or Words or to Provide Erroneous Inputs	Remarks
2a(2). "Cover Fully Open" switch fails in position which erroneously indicated "Open". Short circuit within wiring to computer occurs so erroneous "Open" signal is inputted.	2a(2). Include subroutine in program which will indicate that both "Cover Fully Open" and "Cover Closed" have been received will indicate there is an erroneous input. Separate the connector pins for wires used for "Open" and "Closed" circuits. Present design uses redundant "Open" switches, but both switches are tied to same circuit to controller. Provide separate circuits to controller and incorporate routine to compare inputs. If they differ, compare to similar arrangements and output of routine for "Closed" circuits, or automatically inhibit firing.	2a(2). Routine to abort firing if computer receivers both "Cover Fully" signals.	2a(2). Operator cannot affect this action.	2a(2). Designer may want to analyze time factors for new comparison routine to insure it does not unduly delay capability. It would be beneficial to classify processing of this routine as a critical instruction so a subroutine will be included to insure avoidance of errors.
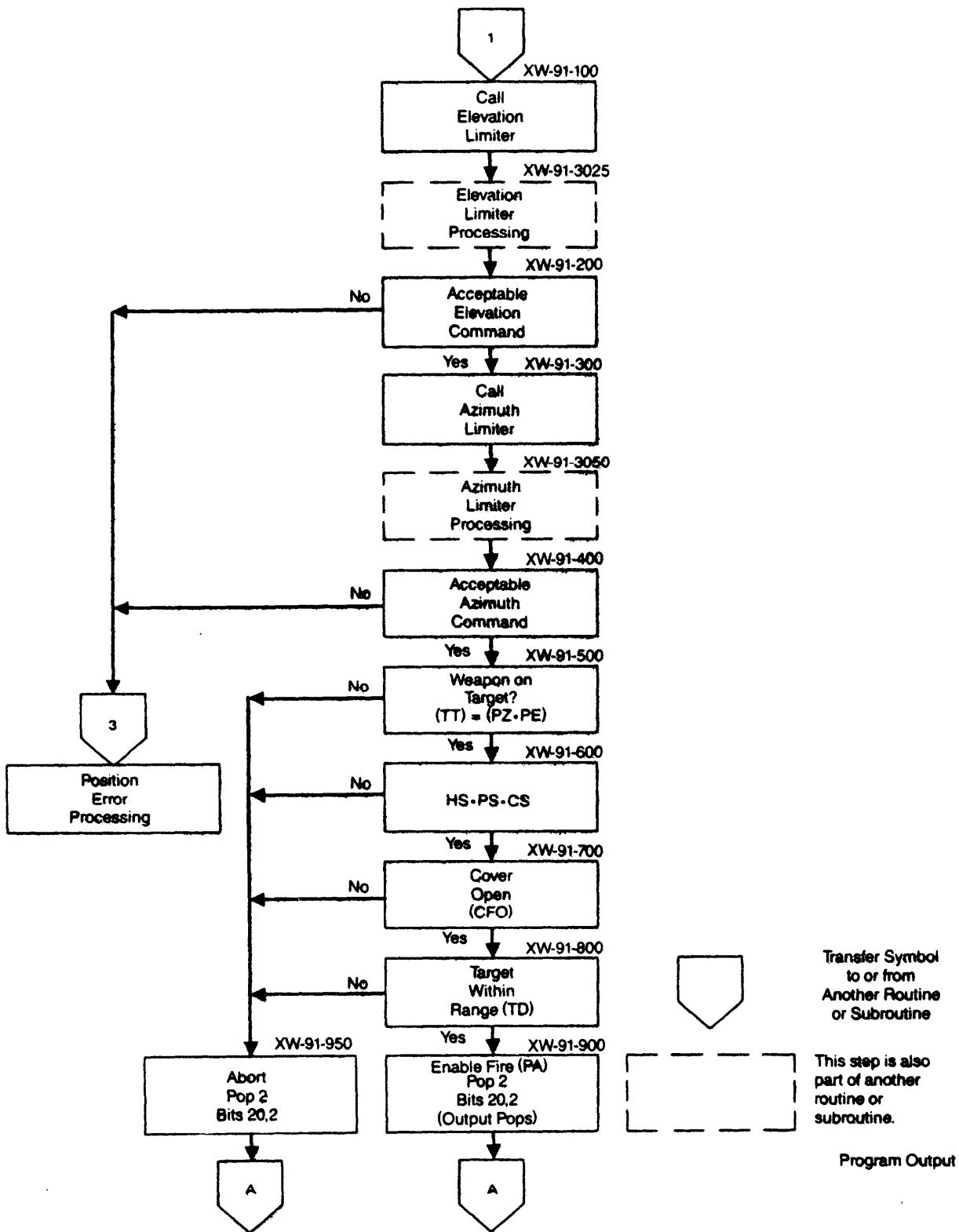
Figure 7-9. XW-91 Computer Software Routine

other items included in the abort relationship—TT, TD, HS, and PS—are not involved with safety. TT and TD were included to abort firing so that weapon system resources, such as ammunition, would not be wasted. $\overline{HS}$ and $\overline{PS}$ indicate failures that would prevent system operation.

Also not shown is the subroutine for processing all the inputs to step XW-91-700.

7-6.4 ANALYSIS

The XW-91 Air Defense System is a complex system that must first be analyzed to determine the potential accidents that might result from controller failures. For that purpose see Tables 7-4 and 7-5; their column headings and meanings are described in par. 7-4.2.

Column 1, Table 7-4, lists the units that are computer controlled. The remaining units in the system need not be subjected to software analysis. The information in Columns 2 and 3, relating to the adverse events and their potential effects, can frequently be derived from a PHA. Data to be entered in Columns 4 and 5, identifying the erroneous computer output signals, and the safeguards can sometimes be derived from an FTA developed specifically for this purpose. The end result of a complete initial software safety analysis of the entire system would be an analysis report similar to Table 7-4, Part 1, but including all units that are computer controlled. From such a report all the safety aspects of a software system that should be analyzed further can be identified.

Early accomplishment of Table 7-4, even without Column 4—which requires information that may not be available when a software analysis is conducted early in the acquisition process—can provide guidance for software programmers. At this stage of software development, the programmers may not have considered the potential hazards that could result from inadequate software programs or routines or from software failures.

Table 7-5 is used for the detailed analysis of a specific potential problem revealed by Table 7-4. Table 7-5 also may contain information derived from other sources. For example, the first item in Column 6 may be derived from a subsystem hazard analysis.

Information from other columns in this detailed analysis may be included in plans for controller tests. If the software program in this example is modified as indicated in the first items of Columns 8 and 11, simulated test inputs can be used to insure that the control system works properly.

Information from this analysis can also be provided to system and subsystem designers and software programmers to incorporate safety-critical items into the design. The second and third items in Column 13 list design features that should be included in the system, but these will be beneficial only if the software program includes provisions to use the inputs.

Each step in the software safety analysis that determines whether or not there can be a deviation from the desired program is subjected to a detailed review, which uses "clues" similar to those in sneak circuit analysis. For example, a review could reveal that a safe, programmed

address in the computer is only one bit different from an address that could generate an unsafe occurrence. The result of that analysis would be a recommendation for a wider separation of those addresses.

The analysis should also determine the adequacy of the software. For example, if the XW-91 Air Defense System turret used only a resolver to determine where the line of sight (LOS) of the weapon pointed, the controller would not know where the LOS was pointing if the resolver or its circuitry failed. If the software program was amended so that the controller also calculated the LOS by integrating rate, time, and direction of turret movement, a second determination could then be made. Thus if the calculated LOS agreed with the indicated LOS of the resolver, it would be apparent that the resolver was working and was correct. If there was a difference, possibly the resolver and its circuitry had failed, and firing would be inhibited. Thus control of a hazard would be exercised by computer software programming.

A software program feature that analysts should be aware of is covered in the second comment in Column 11, regarding TMTT (Tell Me Three Times). For such controller functions the safety analyst is interested primarily in the software in the category of "real time process" control (in contrast with other classes of processing such as scientific analysis and simulation). The routines of interest for safety purposes are iterated and reiterated many times per second.

In general, real time process control software is very insensitive to single-cycle (transient) out-of-limit situations, i.e., errors. If such an error does occur, the condition will be corrected on the next iteration and the transient error is ignored. The iteration time is selected to prevent transient errors—such as those induced by positive or negative peaks—from degrading overall system performance. A question of critical importance then arises regarding how many iterations must contain the out-of-limit signal before the program accepts that a hazardous condition exists and requires control action. Any inhibit function that can be triggered by a single-cycle, erroneous signal is vulnerable to transients—an undesirable situation from the system safety viewpoint. In the initial phases of system design, part of the software safety analysis must be directed toward recognition and elimination of any routine that results in a control action because of single iteration indications that unsafe conditions exist. To correct that weakness in software design, the analyst should recommend the use of the TMTT, 2 3 (two out of three), 3/3 (three out of three), or other processing and verification features.

7-7 ADVANTAGES

Software programs for the control of hardware and or for input to human operators can have major unwanted safety influences on the hardware and on the human operator's decisions. Use of the software safety analysis will reduce the possibility that errors or omissions in the software program design will cause "unplanned modes of operation, unexplained problems, and unrepeatable

glitches or abnormalities in electrical hardware and software systems." (Ref. 12).

The use of SSA techniques and associated techniques described in this chapter will help the safety analyst to compare the software design with the original software specification to insure minimum software errors and omissions and to recommend software and/or hardware changes that will correct the identified deficiencies. Similar checks and controls have been incorporated into software programming after the need for such safeguards was established. Fig. 7-9 has indicated how such needs can be established by the designer. The designer can then indicate to the programmer the need for a safeguard in the computer programming.

7-8 LIMITATIONS

The software safety analysis technique was developed very recently and has not yet been used often enough to determine its effectiveness. To perform a detailed software safety analysis, such as the one described, is a lengthy effort. It cannot yet be performed on computers; it must be done manually. Therefore, its cost of accom-plishment can be high unless it is performed on only a limited number of selected events.

Software design changes at any point must be subject to "configuration control". If any changes are made in a program for any computer-controlled unit that is considered safety critical, those changes should be subjected to immediate reviews to determine that the software programming has not been affected adversely. Such adverse effect could be the removal of an existing program step that contains a safeguard, or it could be the failure to provide a safeguard in a new program. Ref. 11 can be used as a guideline for configuration control of changes.

Some kind of safety-related configuration control method must be used since there is a possibility that seemingly insignificant software changes can have (and have had) major, unforeseen impacts on a system. Such changes can result from late software design; alterations during or after testing; changes made prior to delivery of operational units to using organizations; or changes made in the field for whatever performance, maintenance, or logistic reasons. Regardless of where these changes occur, a safety analysis must be made to insure that the change will not have any hazardous consequences.

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

2. MIL-S-52779A, *Software Quality Assurance Program Requirements*, 1 August 1979.

3. DOD-STD-1679A, *Weapon System Software Development*, 22 October 1983.

4. C. A. Ericson, II, "Software and Software Systems", Boeing Computer Services Company.

5. D. R. Parks, LTC, Letter from Commander, Test and Evaluation Command, DRSTE-CM-R11, Aberdeen Proving Ground, MD, to PM-M60, Tank Program, DRCPM-M6011, Warren, MI, 9 April 1979.

6. Paul Goldsbrough, *The Bugbook IV*, Howard W. Sams and Co., Inc., Indianapolis, IN, 1979.

7. B. W. Boehm, "Software and Its Impact: Quantitative Assessment", *Datamation*, 48-59 (May 1973).

8. G. J. Myers, *Software Reliability, Principles and Practices*, John Wiley and Sons, Inc., New York, NY, 1976, p. 310.

9. R. L. Glass, *Software Reliability Guidebook*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1979.

10. S. L. Gerhart and L. Yelowitz, "Observations on the Fallibility in Applications of Modern Programming Methodologies", IEEE Transactions on Software Engineering SE-2, 195-207 (1976).

11. Saul I. Gass, *Computer Model Documentation: A Review and an Approach*, NBS Special Publication 500-39, National Bureau of Standards, US Department of Commerce, February 1979, p. B-17.

12. James L. Vogas, *Verification of Hardware/Software Integration Through Sneak Analysis*, The Boeing Aerospace Company, Houston Operations, P. O. Box 58747, Houston, TX, 1981.

13. Fread E. Kattuah, "Applicability of System Safety Methods to Software/Firmware Safety", Lockheed Missiles and Space Co., Inc., Sunnyvale, CA.

BIBLIOGRAPHY

National Bureau of Standards, FIPS Pub 38, *Guidelines for Documentation of Computer Programs and Automated Data Systems*, US Department of Commerce, February 1976.

Institute of Electrical and Electronics Engineers (IEEE), *Program Testing Techniques*, Computer Software and Applications Conference, 1977.

A. M. Lister, *Fundamentals of Operating Systems*, The MacMillan Press, Ltd., London and Basingstoke, England, 1975.

K. M. Roehr, "Modeling of Computer System Performance During Development", *Measuring, Modeling, and Evaluating Computer Systems*, North Holland Publishing Company, 52 Vanderbilt Avenue, New York, NY 10017, 1977.

Dennie Van Tassel, *Program Style, Design, Efficiency, Debugging, and Testing*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1974.

Dorothy Walsh, *A Guide for Software Documentation*, Advanced Computer Techniques Corporation, 16 East 32nd Street, New York, NY 10016, 1969.

R. P. Watkins, *Computer Problem Solving*, John Wiley and Sons, Inc., New York, NY, 1974.

Nancy G. Leveson, "Software Safety from a Software Viewpoint", Information and Computer Science, University of California Irvine, Irvine, CA.

David B. Cazden, "Software Sneak Circuit Analysis as a Support Tool", General Dynamics, Convair Division, San Diego, CA.

J. G. Griggs, II, "A Method of Software Safety Analysis", Martin-Marietta, Denver Aerospace, Denver, CO.

CHAPTER 8
OPERATING AND SUPPORT HAZARD ANALYSIS

Two methods are presented for analyzing a system to identify hazards that could be present during specific operational activities. The first method provides analyses to insure that the procedures developed for or by user personnel will contain minimal hazards. The second method provides analyses to insure that contingencies are minimized and controlled. An example of a procedure analysis and a contingency analysis is illustrated for the Howitzer, Self-Propelled, 155-mm, M109.

8-1 DESCRIPTION AND PURPOSE

Prior to the inception of system safety programs and the development of the operating and support hazard analysis (O&SHA), delivered systems often reflected inadequate considerations of user needs, capabilities, practices and tendencies. Operation and maintenance procedures were predicated on the designer's concept of how the system *should* be operated and not on how the less design-oriented user *might* operate it. Designers failed to observe the legal principle of "foreseeability", i.e., to anticipate ways that equipment operators would be endangered by the use or failure of the equipment or by "misuse" of the equipment. O&SHAs are methods whereby designers and analysts can evaluate the prescribed (and possible alternative) operation and maintenance procedures, foresee potential problems, and take corrective action.

The types of hazards that arise may differ substantially during various operations with the same system. For example, maintenance activities may include welding or exposures to high voltages or pressures and thus may introduce hazards that are not present during operation, storage, or transportation of the system. The equipment itself may remain the same during these various operations, but its configuration, the procedures used, the presence of hazardous materials, or the environment will probably be different. For example, if a vehicle is stored without its highly flammable fuel, then storage will constitute a less hazardous situation than operation. Thus any analysis of a particular type of system operation must consider the specific factors involved.

There are two categories of O&SHA, i.e., procedure analysis (par. 8-2) and contingency analysis (par. 8-3). The procedure analysis is an evaluation of the adequacy of the various types of operating procedures. The contingency analysis is a study of operational situations that could develop into emergencies and ways to prevent that from happening. Each method can be applied equally well to all types of operations.

Ref. 1 indicates that the O&SHA is beneficial in

1. Isolating hazardous operations from other activities, areas, and personnel

2. Providing control measures if failures would adversely affect the system or could cause a catastrophic event through injury to personnel or equipment damage

3. Designing, locating, and arranging equipment components so that personnel will not be exposed to hazards—such as electrical shock, cutting edges, and toxic atmosphere—during operation, maintenance, repair, or adjustment

4. Avoiding unnecessary exposure of personnel to physiological and psychological stresses that might cause errors leading to injuries

5. Installing effective standardized warning systems on hazardous components, equipment, etc., for the protection of personnel.

8-2 PROCEDURE ANALYSIS

For purposes of this analysis, assume that the Army materiel has been developed and tested and is now to be delivered to the user organizations. The various operations to which this equipment will be subjected include events such as transportation, storage, training, full operational use, maintenance, repair, testing, and modification. Most of the considerations in an O&SHA will generally review

1. The procedures by which the equipment will be used or could be misused

2. The consequences of material or procedural human failures

3. The means whereby the consequences and failures can be minimized.

8-2.1 DESCRIPTION AND PURPOSE

A complete O&SHA consists of two major phases, i.e.,

1. Phase 1. This phase involves the study of

a. The designer's concept of how a specific piece of equipment should be operated

b. Whether the operator or any other person will be subjected to any hazard while the equipment is being operated as designed

c. The consequences that might result if a material or procedural human failure should occur during accomplishment of any operational or support procedure.

The purpose of this first-phase analysis is confirmation that the operating and support procedures developed by the designer will minimize the probability of injury to the operator and of damage to the equipment. Alternatively, it may be found that even when the designer-specified procedures are followed, unacceptable hazards are present. If so, the procedures, the equipment design, or both, must be changed before proceeding to the next step.

2. Phase 2. This phase is based on the fact that operators sometimes deviate from the procedures established by the designers and take unauthorized actions (which the operators may view as shortcuts) unforeseen by the designers. These potential alternative actions, or misuses, must be investigated since they may lead to mishaps. Therefore, to control any hazardous alternative actions, it is necessary that designers and analysts be able to foresee the alternative actions that can be taken and the consequences they might cause.

Both phases for analyzing operational procedures can be employed while the designers are preparing their operating and support procedures or after they have finished.

8-2.2 ANALYSIS TECHNIQUE AND FORMAT

Because the procedure analysis method is a two-phase process, the techniques and formats for the two phases will differ. The technique and format for Phase 1 are primarily useful for broad evaluations of activities such as system operation, maintenance, test, transportation, handling, and storage. The technique and format for Phase 2 are used for reviewing the detailed step-by-step procedures to determine whether each procedure is adequate and to evaluate probabilities that personnel might deviate from the actions stipulated by designers.

8-2.2.1 Phase 1 Analysis
8-2.2.1.1 Technique for Phase 1

As stated in the beginning of par. 8-2.1, the technique involves examining the designer-prescribed concepts for operating the materiel. If this procedure analysis is done after the operating and support procedures have been prepared, the analysis can proceed in a straightforward manner. However, if the procedure analysis is to be made prior to ordering the preparation of the operating and support procedures, the analysis can only be accomplished with designer assistance. Regardless of its source, information for analysis must be subjected to simple, systematic integration and study as follows:

1. Ref. 2 points out that the first task in the analysis of a specific job is to separate it into its basic steps. Therefore, for each step or activity, describe briefly what is to be done and record it. Use the same order in which the steps are to be performed.

2. Examine each step to identify hazards or potential accident sources that could result from accomplishment of that step.

3. Develop solutions to eliminate or control the hazards.

8-2.2.1.2 Format for Phase 1

A procedure analysis matrix is shown in Fig. 8-1. It indicates how the three basic tasks previously described can be broken down even further. In Column 1, the operational or support step identifications are correlated to a functional diagram that the analyst prepares in order to identify the operational sequence. This diagram can take the form of a vertically developed logic-type diagram simply to indicate the designer-specified sequence of operating and support procedural steps to be considered in the procedure analysis. Each step will be assigned the identification number from the existing procedure or an identification number arbitrarily assigned by the analyst if no other number exists.

Each operational step is followed by a short description (Column 2) of the step. The information in the next six columns (3 through 8) indicates the sources of the hazards, events that could lead to a mishap, injury or damage that could result, and probability of occurrence. The information in Column 9 often is included to present an indication of the severity of the mishap that might result. Column 10 lists pertinent standards or regulations that may contain measures (Some may be mandatory.) prescribed to control the hazards. Column 11 includes solutions, and Column 12 identifies the organization or person responsible for taking action on the solution.

A narrative format can also be used to present this first part of the procedure analysis. In the narrative, each operational or support step is discussed from the viewpoint suggested by each of the column headings. The discussion of all of those factors can be placed in one paragraph for each operational or support step. For more complex procedural steps, the discussion of each step can be organized into separate paragraphs with major paragraphs identified by title.

Other information that the analyst may wish to include in the matrix is

1. The effect of each recommended action on the hazard category or the probability of occurrence

2. Remarks regarding previous similar mishaps and related events and other pertinent comments or information not included elsewhere

3. Warnings that should be included on equipment, in manuals, and in training courses

4. Status of actions to implement the recommended or required hazard controls.

8-2.2.2 Phase 2 Analysis
8-2.2.2.1 Technique for Phase 2

The technique for Phase 1 emphasized a study of each designer-specified operating or support procedural step to determine whether it could be hazardous due to the materials and the action involved in that step. The emphasis in Phase 2 combines the evaluation of designer-specified procedures with a study of reasonably foreseeable unauthorized alternative procedures that operational personnel might choose to employ. This technique is designed to consider systematically these alternative possibilities, their consequences, and ways to reduce the risk of the consequences as follows:

1	2	3	4	5	6
IDENTIFICATION NUMBER	OPERATIONAL STEP	HAZARDOUS ELEMENT	HAZARDOUS CONDITIONS	TRIGGER EVENT	POTENTIAL FAILURE

7	8	9	10	11	12
PROBABILITY OF OCCURRENCE	EFFECT OR CONSEQUENCES	HAZARD CATEGORY MIL-STD-882	REFERENCE STANDARD OR REGULATION	PREVENTIVE OR CORRECTIVE ACTION	WHO TAKES ACTION

Figure 8-1.   Suggested Format for Phase 1—Procedure Analysis

1. List each step in the procedure that the designer expects the operational personnel to follow. Note that designers frequently include multiple actions in one procedural step; however, the analyst must review each action separately. For example, the loading procedure for a 155-mm howitzer states: "Make sure round is clean and fuze is present and fully seated." (Ref. 3). This statement involves three separate actions that must be considered:

    a. Make sure the round is clean.

    b. Make sure the fuze is present.

    c. Make sure the fuze is fully seated.

2. List ways the operational personnel might deviate from the action stipulated by the designer and, instead, undertake alternative actions.

3. Indicate the potential effect(s) that might result if an alternative action is undertaken. If the potential effect will not result in, or contribute to, injury or damage, it need not be investigated further.

4. If an alternative action could potentially generate or contribute to a mishap, the analyst should list any measures that might be incorporated in the design or the procedure to avoid or lessen the possibility of that alternative action.

5. If the possibility of that alternative action cannot be eliminated, the analyst should list possible measures to avoid or minimize the adverse effects of the potential mishap.

6. Under "Remarks" include any omissions, ambiguities, or other deficiencies in this procedure. Also include any other pertinent information regarding past experiences and lessons learned.

7. A column can be included to list any warnings, cautions, or other notes that should be incorporated into manuals, other instructional material, or labels on the equipment.

8-2.2.2.2 Format for Phase 2

The format for Phase 2 is the logical way to present the information developed by means of the technique for Phase 2—evaluating both the designer-specified procedures and possible unauthorized procedures that operational personnel might devise. See Fig. 8-2 for an example of the format for Phase 2. A detailed procedure analysis of the loading procedure for the Howitzer, Self-Propelled, 155-mm, M109, is used to illustrate this technique. (See par. 8-2.4.) A discussion of the columns of Fig. 8-2 follows:

1. Column 1 identifies the procedural step by number from the operator's manual.

2. Column 2 identifies the wording of the step exactly as written in the operator's manual.

3. Column 3 lists foreseeable unauthorized alternative actions. These might consist of a failure to perform the stipulated action (omission), a failure to accomplish it completely, or action to change the prescribed step.

4. Column 4 indicates the potential effects that might result from the deviations.

5. Column 5 recommends measures to preclude the operational personnel from devising alternative procedures that could cause mishaps.

6. Column 6 lists any measures that should be taken to avoid or minimize any potential damage or injury from mishaps that cannot be forestalled.

7. Column 7 will include any pertinent comments not included elsewhere.

8. Column 8 lists any recommendations for warnings or cautions to be included in operation and maintenance manuals or equipment labels.

The format illustrated in Fig. 8-3 has used a separate sheet for each procedure. Some analysts may prefer to list all procedures consecutively. In that case, the table should contain an extra column following the procedure number to list the title of each procedure.

The analyst also may wish to include an additional column for risk assessments; it would estimate the probability that each alternative action might occur. To develop such probabilities, he would draw upon any data from related field experience and detail the frequency with which specific deviations have occurred.

8-2.3 SOURCES OF DATA

Probably the best source of data for a procedure analysis is experience. This is particularly true for categories of materiel such as artillery with which the Army has had long experience.

If "experience" data are unavailable from predecessor systems, the safety engineer may simulate them by having personnel execute the proposed procedures using a mockup or a prototype. The test objectives are twofold: (1) to determine whether the specified procedures can be performed safely and (2) whether the test personnel can substitute any potentially hazardous unauthorized alternative procedures.

Remember that this part of the procedure analysis deals with human reactions in performing specified procedures. When the safety analyst can reasonably suspect that any human action will deviate in some manner from the specified action, an error is possible. One method of classifying such errors categorizes them as persistent or random. Persistent errors will recur under similar conditions. Any repeating condition that is contrary to the normal human desire for less physical and mental effort, avoidance of discomfort, and working slowly will contribute to persistent errors.

Random errors are caused by randomly encountered conditions such as the physical and mental health of the operator or transient physical environments to which he may be exposed. Whether a random situation is important to the procedure analysis will depend on the severity of the consequences of the human error resulting from the situation.

Error probability data for specific task elements can sometimes be obtained from the Data Store developed by the American Institute for Research (Ref. 4). Refs. 5 through 7 are papers that contain quantitative data on human reliability and probabilities of errors, and they contain methodologies on how to compute probabilities that a programmed sequence will be accomplished successfully.

1	2	3	4	5	6	7	8
MANUAL IDENTIFI-CATION NUMBER	DESIGNATED ACTION DESCRIPTION	POSSIBLE ALTERNATIVE ACTIONS	POTENTIAL EFFECTS OF ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID EFFECTS OF ALTERNATIVE ACTIONS	REMARKS	WARNINGS AND CAUTIONS

Figure 8-2. Suggested Format for Phase 2—Procedure Analysis

System: Howitzer, Self-Propelled, 155-mm, M109
Procedure: Loading and Firing

1	2	3	4	5	6	7	8
MANUAL IDENTIFICATION NUMBER	DESIGNATED ACTION DESCRIPTION	POSSIBLE ALTERNATIVE ACTIONS	POTENTIAL EFFECTS OF ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID EFFECTS OF ALTERNATIVE ACTIONS	REMARKS	WARNINGS AND CAUTIONS
4.20a	Make sure round is clean and fuze is present and fully seated.	1. Cannoneer does not insure round is clean, and dirt is present.	1a. Small amount of dirt would not permit round to seat properly, which would permit gas from propelling charge to escape so that a short round results. 1b. A large amount of dirt might cause an obstruction in the bore so that an overpressure condition would result, which could burst the tube.	1. Specific cannoneer designated to make certain round is clean. Person inserting fuze can also make sure round is clean because presence of dirt may preclude fuze from becoming fully seated. All persons handling or storing projectiles should be made aware of need to keep projectiles clean.	1. No practicable actions to avoid effects of a short round except that attempts be made to avoid firing over friendly troops.	1. Cannoneers should be instructed in proper procedures and told that no deviations will be permitted. Intensive practice should be carried out so that following proper, designated procedural steps become a habit. Section Chief should observe actions of cannoneers to insure that designated procedures are followed without deviations. Where deviations occur, correct the cannoneer immediately.	1. Include warning in instructions of importance to insure that round is clean.
		2. Cannoneer fails to check that fuze is present, and it is not.	2. If the nose plug has been removed, a fuze not inserted, and the projectile is loaded, then there is a potential for the supplementary charge to fall out of the projectile. When the gun is fired, the supplementary charge would be initiated by the friction induced between the projectile and the cannon wall. The energy from the supplementary charge will induce an in-bore explosion. Although the potential for the hot propellant gases detonating the supplementary charge cannot be ruled out, the probability of this happening is very remote.	2. Specific cannoneer designated to insure fuze is present and tightly seated. Determine whether two-man concept can be employed: have designated cannoneer call out "Fuze Present" after he checks.	2. No practicable action to avoid effects of having projectile fired with no fuze.	2. Two-man concept (from nuclear weapon activities) is the idea that a second person, who may not be as knowledgeable, insures that first person has accomplished a stipulated step in a task. Observe remarks under 1.	2. Include warning in instructions of need to insure that check must be made to insure fuze is present on projectile.

Figure 8-3.   Procedure Analysis for Howitzer, Self-Propelled, 155-mm, M109

System: Howitzer, Self-Propelled, 155-mm, M109
Procedure: Loading and Firing

1	2	3	4	5	6	7	8
MANUAL IDENTIFICATION NUMBER	DESIGNATED ACTION DESCRIPTION	POSSIBLE ALTERNATIVE ACTIONS	POTENTIAL EFFECTS OF ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID EFFECTS OF ALTERNATIVE ACTIONS	REMARKS	WARNINGS AND CAUTIONS
4.20a		3. Cannoneer fails to check that fuze is fully seated, and it is not.	3. In cases where a long intrusion fuze is used (fuze with a long stem), the setback force has been known to push the fuze sufficiently deep into the projectile so as to induce detonation.	3. See 2. In the event the cannoneer is to call out after he checks the fuze, he should call, "Fuze Present and Fully Seated."	3. No practicable action to avoid effects if fuze is not fully seated.	3. If a second cannoneer is to check that the fuze is at least hand tight, he should make the same statement. Observe remarks under 1.	3. Include warning to insure fuze is tight.
4.20b	Make sure there are no obstructions or burning propellant in the tube. After each round is fired, the tube is swabbed with water and checked to insure there is no burning propellant in it.	Designated cannoneer fails to inspect tube, so obstruction is not detected or removed.	Firing a round with an obstruction in the tube can cause an in-bore, premature explosion.	Two-man concept, with a second cannoneer to check bore. Call out "Tube Clear" after checking.	No practicable means.	See 1 under 4.20a.	Include suitable warning in instruction.
4.20c	Check cannon firing lock to see that primer expended in previous firing has been removed.	Cannoneer fails to make check.	No safety effect.	Provide automatic ejection of primer case when breechblock is opened.	None required.	Extraneous words in proposed instructions "cannon firing lock to see" can be eliminated. No instruction is included in the procedure regarding action to be taken if primer for previous firing has been expended or cartridge case removed.	1. Include warning or note on action to be taken if primer has not been expended or cartridge case not removed. 2. If the primer from a previous round is not expended, there is a misfire. In the event of a misfire, the breech must not be opened until certain misfire procedures have been taken.
4.20d	Remove grommet from projectile.	Cannoneer fails to remove grommet.	Projectile cannot be inserted or seated, so there will be no room to insert propellant charge. No safety effect.	Good training, intensive practice, and close surveillance.	None required.		

Figure 8-3.   (cont'd)

System: Howitzer, Self-Propelled, 155-mm, M109
Procedure: Loading and Firing

1	2	3	4	5	6	7	8
MANUAL IDENTIFICATION NUMBER	DESIGNATED ACTION DESCRIPTION	POSSIBLE ALTERNATIVE ACTIONS	POTENTIAL EFFECTS OF ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID EFFECTS OF ALTERNATIVE ACTIONS	REMARKS	WARNINGS AND CAUTIONS
4.20e	Load fuzed projectile into tube and ram it solidly into the firing chamber.	1. Cannoneer fails to load projectile into tube(s). 2. Cannoneer fails to ram projectile into the firing chamber, so it is not wedged into the forcing cone.	1. Fire bolt will be generated if firing occurs without projectile. 2. May result in very short round.	Same as 4.20d	1. No practicable means except cannoneer calls out after action has been completed. 2. No practicable means except cannoneer calls out after action has been completed.	Comment from person experienced with this type of weapon indicated that a fatal accident occurred when the weapon was fired at a high angle without the projectile. Fireball killed the crew.	
4.20f	Remove the igniter protective cap from propelling charge and load propelling charge into cannon chamber, with igniter (red bag) toward the breech.	1. Cannoneer fails to remove the igniter protective cap. 2. Cannoneer fails to load propelling charge into chamber. 3. Cannoneer loads propelling charge with igniter (red bag) toward the projectile.	1. No ignition of propelling charge. Will have to carry out misfire procedure. 2. No propelling charge to ignite. Will have to carry out misfire procedure. 3. No ignition of propelling charge or possibly a hangfire. Will have to carry out misfire procedure.	Same as 4.20d.	1. Carry out misfire procedure. 2. Carry out misfire procedure. 3. Carry out misfire procedure.		
4.20g	Close and lock the breechblock.	Cannoneer fails to close and lock the breechblock completely either because of error or presence of dirt.	1. If breechblock is wide open, the primer will not reach the igniter, and there will be no further action. 2. The weapon cannot be fired if the breechblock is not locked. If the breechblock is not locked and the propellant is ignited in some manner other than the normal primer, the pressure generated will burst open block with possible injury or death to crews.	1. Training, intensive practice, and close supervision. Cannoneers must insure that marks of breechblock are aligned properly to indicate it is closed	1. Gun crew members could be in positions where a mishap would not result in injuries to them.	1. Mechanism to prevent firing unless breechblock is fully closed and locked could be designed but may be too delicate for such heavy use.	1. Insert warning in instructions regarding need to insure alignment of breechblock marks before primer is inserted.

(cont'd on next page)

Figure 8-3. (cont'd)

System: Howitzer, Self-Propelled, 155-mm, M109
Procedure: Loading and Firing

1	2	3	4	5	6	7	8
MANUAL IDENTIFI-CATION NUMBER	DESIGNATED ACTION DESCRIPTION	POSSIBLE ALTERNATIVE ACTIONS	POTENTIAL EFFECTS OF ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID ALTERNATIVE ACTIONS	MEASURE(S) TO AVOID EFFECTS OF ALTERNATIVE ACTIONS	REMARKS	WARNINGS AND CAUTIONS
4.20h	Insert primer, and move firing lock to firing position.	1. Primer is not inserted. 2. Firing lock is not moved to firing position.	No ignition of propelling charge.		No safety effect.	This procedure does not include instruction for gun crew positions so they will not be hit when the gun recoils. This procedure does not provide instruction when to fire. Should be preceded by instruction that all cannoneers are to be in positions clear of path of recoil.	Provide warning that primer is not to be inserted unless the breechblock is closed and locked. Provide warning that command to FIRE is not to be given unless all cannoneers are clear of recoil path.

Figure 8-3. (cont'd)

MIL-HDBK-764(MI)

8-2.4 EXAMPLE

The data (Ref. 3) provided in Fig. 8-3 are the result of a procedure analysis using information from Ref. 2. Each step in the operation of loading and firing the Howitzer, Self-Propelled, 155-mm, M109, is considered in the analysis. Both the normal procedures and possible errors and or omissions are evaluated for hazards. A common expression for this technique is the "what if..." examination to discover anomalies in the procedures that can be related to hazardous conditions.

8-2.5 ADVANTAGES

The procedure analysis will either confirm that the system will be operated safely or will identify areas of the design that will induce unsafe operation. In the worst case it will identify operations that cannot be considered safe.

In normal acquisition programs the designers should have the assistance of logistic and using command experience to avoid unsafe procedures. However, it sometimes happens that the transfer of a functional requirement into hardware results in the development of safety-unacceptable procedures. The safety procedure analysis is most useful for discovering this area of the design and its associated unsafe procedures. Through the systematic study of each step of each operational procedure, other non-safety-related errors and omissions will be discovered. These findings are a fringe benefit because they are also important to the correct operation of the materiel for achieving maximum efficiency in user organizations.

8-2.6 LIMITATIONS

There are few limitations to the accomplishment of a procedure analysis. The chief ones are the ability of the analyst and the level of detail to which the analysis is to be conducted. Ref. 2 states that most jobs to be analyzed will separate into 10-15 basic steps. However, the tasks considered by Ref. 2 are comparatively simple ones. The example shown in Fig. 8-3 theoretically would involve fewer than 10 steps for the entire loading and firing procedure, but the entire system contains many such procedures. The entire system analysis may be simple to accomplish, but it may also be so lengthy that it represents significant cost. Less detailed analyses will cost less but may not provide the necessary insight to determine the actual points at which human errors could cause accidents.

8-3 CONTINGENCY ANALYSIS

A contingency is considered to exist if a system is not in a normal operating state and conditions are such that an accident might occur unless corrective action is taken immediately. This definition assumes that

1. There is some corrective action that can be taken.
2. There is time to take corrective action before an accident occurs.

8-3.1 DESCRIPTION AND PURPOSE

A contingency will exist if a flammable fuel has been spilled and immediate action is necessary to prevent a fire. Sometimes people confuse "contingency" with "emergency". In a contingency, no accident has yet occurred. In an emergency, an accident may or may not have already occurred.

The contingency analysis should be used for any materiel that could become involved in an accident. Even minor items might be improved through small design changes suggested by a contingency analysis. For example, a laser range detector or illuminator can cause injury to friendly personnel. The AND condition that prevents this event is visual observation of the line of sight. The operator, however, could be momentarily distracted from the sighting operation but still could fire the laser by pulling the trigger. During this moment, a friend might cross the line of fire of the laser and be injured if the laser beam strikes him. To prevent this accident, a brow interlock switch could be installed to prevent firing the laser unless the operator is pressing his brow to the sight for sighting. If there is any possibility that the laser beam can strike a reflective surface, the sight should be equipped with a filter to protect the operator.

In addition to equipment redesign, the contingency analysis may also suggest changes to the operating procedures and the development of emergency procedures. Major systems are generally capable of causing more severe consequences when involved in an accident. These systems, therefore, should benefit in many ways from a contingency analysis by the development of appropriate emergency procedures, identification of containment and/or suppression equipment needs and procedures, identification of escape and rescue equipment needs and procedures, and identification of special training and skill requirements. If other safety analyses have already been completed, the contingency analysis can then confirm that no safety deficiencies in the operating procedures remain in the system. If such deficiencies do remain, the contingency analysis will reveal the necessary changes required.

A contingency exists when one or more, but fewer than all, of the events to an AND gate (See Fig. 8-4.) that lead to the adverse top event in a fault tree is inadvertently present. ("Inadvertently" distinguishes a contingency from a situation in which the AND conditions of a fault tree are satisfied intentionally until only one restraining condition remains. For example, the blocking elements in a fuze for a missile launch may be removed sequentially until only one more required action—pressing the firing button—remains.) In a contingency, the adverse top event, or accident, will occur when the last condition or input event is unintentionally satisfied.

When only one more condition or input event is required to generate an accident and its probability of occurrence is unacceptably high, immediate action must

8-10
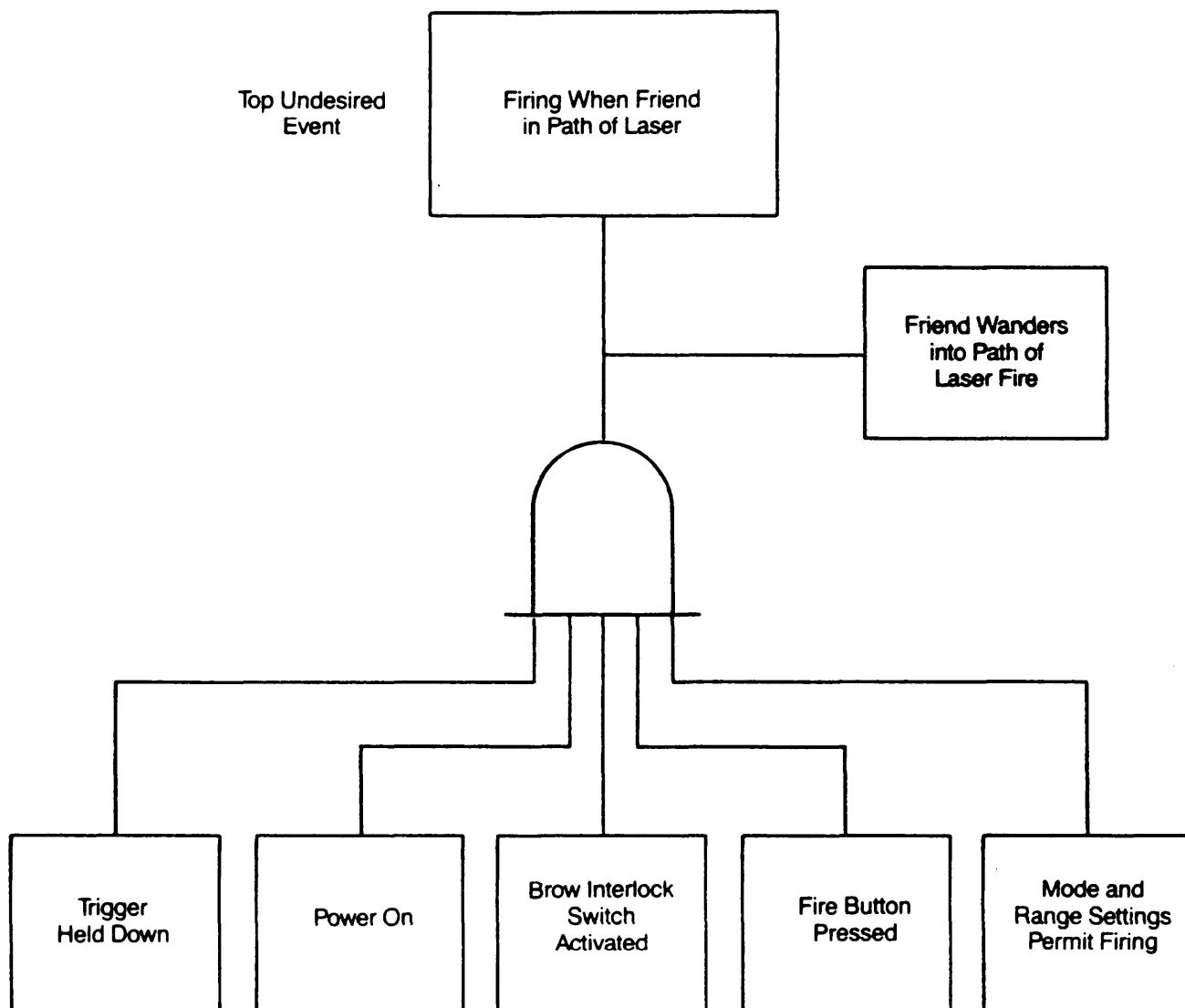
Figure 8-4.   Simple Logic Tree Use for Contingency Analysis

be taken. In a highly energetic system, such as a nuclear weapon, the magnitude of the injuries and damage that would result from an accident generally requires that the design contain a large number of safety features to be unblocked before the top event could occur. The inadvertent unblocking of even one of these safety features might be considered a contingency.

When events are expressed in symbols, in terms of Boolean logic, an undesired event K and the existence of a contingency might be expressed as

$$K = A \cdot B \cdot C \qquad (8\text{-}1)$$

$$\text{Contingency} = A \cdot B \cdot T + A \cdot C \cdot T$$
$$+ B \cdot C \cdot T + A \cdot T + B \cdot T + C \cdot T \qquad (8\text{-}2)$$

where

A, B, and C = events or conditions that contribute to the occurrence of K

T = added condition that development into an accident requires enough time for corrective action to be taken.

Fig. 8-5 illustrates how the Boolean logic equation can be formed from the conditions shown in the logic diagram. Eq. 8-3 expresses the undesired event and the events that lead to the undesired event:

$$K = A \cdot B \cdot C \cdot D \qquad (8\text{-}3)$$

where

A = intentional event that must occur
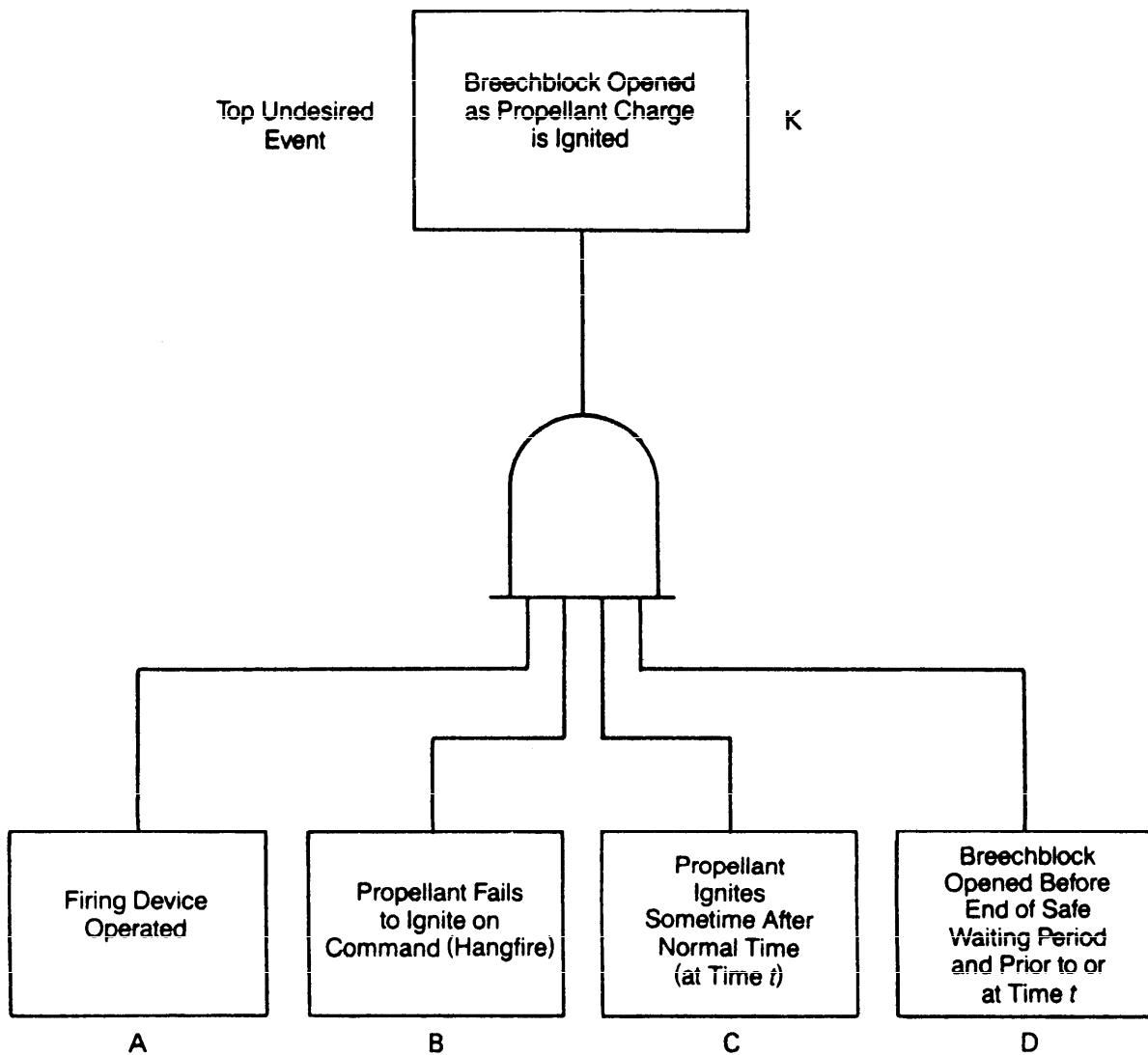
Figure 8-5. Simple Logic Diagram to Illustrate Boolean Equation

B, C = other than normal, unintentional events
   D = correct contingency action, in this instance,
        to prevent the unwanted event if D is taken
        after time t—beyond which the propellant
        can no longer be ignited.

If event D occurs prior to or at time t, an accident will
occur. Although this example is the reverse of the concept
that time t is the period during which corrective action
can be taken to eliminate the contingency, the example
still illustrates that time is a factor. In this case, delaying

the normal event of opening the breechblock is an action
to negate the contingency.

Ref. 8 indicates one way to use fault tree analysis to
determine where monitoring devices might be located to
sense critical information that would indicate the exis-
tence of a contingency. In Ref. 8 the author presents a
mathematical means of computing, from a quantitative
fault tree,

   1. The probabilistic importance of events in an
operation
   2. Where critical sensors should be located within a
system.

8-3.2 ANALYSIS TECHNIQUE AND FORMAT

8-3.2.1 Technique

For maximum usefulness, the contingency analysis technique must employ a systematic method suitable for the evaluation of any type of operation. A contingency analysis of the Howitzer, Self-Propelled, 155-mm, M109, is used to illustrate this technique. (See par. 8-3.4.)

To identify possible contingencies, use clues from Army field experience, accident data, and previously completed safety analyses. The analyst uses the following steps:

1. Select a contingency and evaluate the contingency to determine whether existing emergency procedures are satisfactory to control it. If not, make that contingency the top adverse event of a fault or logic tree. This undesired event will be analyzed the same way as a top hazardous event in a fault tree analysis is analyzed.

2. Identify the conditions and events leading to the undesired top event. Then use the fault tree analysis to identify the factors that can cause those input conditions and events.

3. Establish the combinations of input events that will result in the contingency.

4. Indicate how the existence of the contingency or of each condition of the event leading to the contingency can be recognized, e.g., temperature indicator and pressure gage. Also, identify any alternative indicators to verify the existence of the contingency in case of doubt that the usual indicating device is correct. (That a pressure gage is truly reading a drop in pressure might be confirmed by a decrease in flow indicated by a flow gage or by visually noting an output.)

5. List the actions to be taken to restore control of the hazard. This might involve corrective action to eliminate the problem or preventive action to insure that the contingency does not develop into an accident. For example, closing a valve will prevent leakage of flammable gas into an occupied area, using a blower will reduce the level of gas to less than that required for a flammable mixture, or injecting another gas—such as a fluorocarbon—will prevent combustion.

6. List any other precautionary measures to be taken while a contingency exists. (If a flammable mixture exists, there should be no smoking, open flames, or use of electrical equipment that might cause arcs or sparks in the hazardous atmosphere.)

In addition, the analyst might find it desirable to include columns for the following additional information:

1. *Point of No Return.* When a contingency has occurred, it is often desirable to indicate at what point the effort to save equipment or an operation is to be considered unsuccessful and the persons making the effort should abandon it and seek their own safety. An ammunition fire is a good example of this contingency situation. The fire is one step toward the major unwanted event, i.e., a catastrophic explosion that could level the area.

2. *Time Availability.* Estimate the time required for a contingency to devolve into an accident. An example is the "fallback time" for explosive ordnance engulfed in a fire. These data emphasize the time element; the data in the previous step describe the physical conditions by which on-site personnel determine the point of no return.

3. *Contingency Equipment.* The analyst may list the types of personal protective (and other) equipment that might be used to control the hazards contributing to the contingency and where this equipment is to be located.

4. *Outside Assistance.* Information on outside assistance that might be required or helpful can be listed in this column.

5. *Probability Assessment.* The probabilities that a contingency might occur and that it might devolve into an accident can be listed.

8-3.2.2 Format

The format for a contingency analysis must provide a clear understanding of the possible events leading to the undesired event. The format given in Fig. 8-6 is recommended. A discussion of the columns follows:

1. Column 1 is a description of the potential accident and actions to prevent it.

2. Column 2 is a description of the inadvertent event that will place the system one step (event) closer to an accident. The unintentional unblocking of a safety element in a system is a contingency.

3. Column 3 indicates the possible cause of the contingency. The cause may be materiel failure, personnel error, or a combination of both.

4. Column 4 is the indicator that a contingency has occurred. It contains a brief description of the evidence indicating that the contingency has occurred.

5. Column 5 explains the means of verifying that a contingency has occurred. Any mechanical, electronic, or visual evidence that can be obtained through a safe action should be described. These data augment the information of Column 4.

6. Column 6 indicates the remedial action that must be taken. The description should include reference to the time T during which action can be taken to control the contingency. If T is not known, state any data helpful for determining T or to which it is related.

7. Column 7 lists the means for verifying that the contingency has been controlled. This includes any physical evidence or safe human action to verify that the contingency has been controlled. If time is an element of this verification, the time span or means to determine it should be described.

8. Column 8 is a general description of the safety precautions that should be observed from the time of the first indication that a contingency has occurred.

9. Column 9 provides a place to enter any additional information that is helpful in solving the contingency problem. References to other safety analyses or tests or to other engineering studies might be appropriate.

1	2	3	4	5
ADVERSE EVENT TO WHICH CONTINGENCY MIGHT LEAD	DESCRIPTION OF CONTINGENCY	POSSIBLE CAUSE OF CONTINGENCY	INDICATOR THAT A CONTINGENCY HAS OCCURRED	MEANS OF VERIFYING THAT A CONTINGENCY HAS OCCURRED

6	7	8	9
ACTION TO PREVENT CONTINGENCY FROM DEVELOPING INTO THE ADVERSE EVENT	MEANS OF VERIFYING THAT THE CONTINGENCY HAS BEEN CONTROLLED	PRECAUTIONARY MEASURES	REMARKS

Figure 8-6. Suggested Format for Contingency Analysis

8-3.3 SOURCES OF DATA.

As indicated, much information for contingency analyses can be derived from fault tree analyses. Methods of controlling hazards or of limiting them further frequently can be obtained from manufacturers of safety equipment, many of whom can be found in publications such as Ref. 9.

Reports of accidents that resulted after a contingency period during which corrective action was not successfully undertaken are often indicative of deficiencies that existed in predecessor or contemporary systems. The analyst can obtain useful data from these events. He can also use them to evaluate whether his proposed methods of controlling contingencies would have succeeded in these cases. Par. 2-3 provides additional sources of information.

8-3.4 EXAMPLE

Fig. 8-7 presents an example of an analysis of a contingency that might result during the loading and firing procedure on which the analysis in Fig. 8-3 was based. This example was selected to illustrate that the contingency analysis is interrelated to the procedure analysis. In addition, the corrective procedures developed to control a contingency should undergo a procedure analysis as described in par. 8-2.

8-3.5 ADVANTAGES

This is the first method whereby designers can determine the actions that should be taken to control a contingency. Had the personnel at the Three Mile Island nuclear power plant been provided with the contingency procedures resulting from an analysis such as this, they would have been able to minimize the possibility of an accident and the resulting effects.

8-3.6 LIMITATIONS

There is no limitation of the contingency analysis itself. It is possible to make this analysis as thorough as any other safety analysis; it depends only on the information available and on the skill, experience, and imagination of the analyst in developing descriptions of nonnormal operational events. To this end, the more contact the analyst can have with organizations using similar Army materiel, the better the contingency analysis will be.

REFERENCES

1. R. J. Firenze, "Systems Approach Extracts Hazard Data From Production Operations", *National Safety News*, 54-60 (1972).

2. J. E. Rankin and M. G. Zabetakis, *Job Safety Analysis, Safety Manual No. 5*, Mine Enforcement and Safety Administration, US Department of the Interior.

3. TM-9-2350-217-10N, *Operator's Manual for Howitzers, Medium, Self-Propelled: 155-mm, M109, M109A1, and M109A3*, 29 December 1978.

4. S. J. Unger, R. W. Smith, and D. Payne, *An Index of Electronic Equipment Operability: Data Store*, Report AIR C43-1/62-RP(1), American Institute for Research, Pittsburgh, PA, 1962.

5. A. M. Stave, *The Quantification of Human Reliability*, TIS65SD216, Valley Forge Space Technology Center, General Electric Company, Philadelphia, PA, March 1965.

6. L. W. Rook, Jr., *Reduction of Human Error in Industrial Production*, Report SCTM 93-62(14), Sandia Corporation, Sandia Base, NM, June 1962.

7. A. D. Swan, *A Method for Performing a Human Factors Reliability Analysis*, Sandia Corporation Monograph SCR-685, Sandia Corporation, Sandia Base, NM, August 1963.

8. H. E. Lambert, *Fault Trees for Location of Sensors in Chemical Processing Systems*, UCRL 78442, Lawrence Livermore Laboratory, Livermore, CA, July 1976.

9. *Best's Safety Directory*, A. M. Best Company, Morristown, NJ, Latest edition.

BIBLIOGRAPHY

MIL-M-81273A, *Manuals, Technical, General Specifications for*, 26 April 1966.

W. E. Tarrants, *Utilizing the Critical Incident Technique as a Method for Identifying Potential Accident Causes*, US Department of Labor, 1963.

D. Freund and J. T. Hawkins, *The Delphi Technique: A New Approach to Shipboard Hazard Identification and Ranking*, Weapons System Safety Symposium, Naval Weapons Laboratory, 16 May 1972.

S. H. Dole, et al., *Contingency Planning for Space Flight Emergencies*, Memorandum RM-5200-NASA, The RAND Corporation, Santa Monica, CA, January 1967.

1	2	3	4	5
ADVERSE EVENT TO WHICH CONTINGENCY MIGHT LEAD	DESCRIPTION OF CONTINGENCY	POSSIBLE CAUSE OF CONTINGENCY	INDICATOR THAT A CONTINGENCY HAS OCCURRED	MEANS OF VERIFYING THAT A CONTINGENCY HAS OCCURRED
Injury or death to gun crew because of delayed recoil caused by delayed firing.	A failure to fire may be due to a hang-fire. If a cannoneer moved to open the breechblock and the propelling charge ignited, he might be injured or killed by the recoil.	1. Propelling charge inserted with red bag toward projectile and not toward breech. 2. Faulty primer. 3. Failure to remove igniter protective cap. 4. Wet propelling charge.	Weapon did not fire.	Attempt to fire weapon two additional times. a. Wait two minutes after each attempt to fire. b. Remove and examine primer. c. If primer has fired, insert new one and try again. d. If primer has not fired, replace primer or firing mechanism component.
Injury or death to gun crew by back-blast when breechblock is unlocked or open.	A failure to fire may be due to a hang-fire. If the breechblock is unlocked or opened and the propelling charge is ignited, the backblast, which would occur, could kill or severely injure anyone in the immediate vicinity of the rear of the gun.	Same as above.	Same as above.	Same as above.

6	7	8	9
ACTION TO PREVENT CONTINGENCY FROM DEVELOPING INTO THE ADVERSE EVENT	MEANS OF VERIFYING THAT THE CONTINGENCY HAS BEEN CONTROLLED	PRECAUTIONARY MEASURES	REMARKS
1. Evacuate all personnel but chief of section and No. 1 cannoneer. 2. Stand clear of recoil path. 3. If round is not fired or removed in six minutes, evacuate all personnel from weapon and notify support personnel.	1. Weapon fired. 2. Propelling charge and projectile removed from weapon.	All failures to fire should be treated as hangfires, with the idea that weapon firing will occur after a time delay.	See procedure analysis for situations that could result in failures to fire. Each failure to fire should be treated as a contingency.

Figure 8-7. Contingency Analysis for Howitzer, Self-Propelled, 155-mm, M109

PART THREE
GENERAL DESIGN REQUIREMENTS
CHAPTER 9
CONSIDERATIONS FOR GENERAL DESIGN APPLICATIONS

Different methods of eliminating and controlling hazards that could lead to accidents are presented in descending order by degree of effectiveness. Fail-safe designs and isolation techniques are discussed as a means of preventing injury and damage. Reliability technology is discussed in terms of minimizing failures. Safety factors, warning devices, and labeling are presented in sufficient detail for the reader to understand how these techniques are applied in safety considerations. Planning and equipping for escape, rescue, and survival— important considerations for a well-prepared organization—are discussed. The chapter concludes with a discussion of test conditions involving the safety aspects of test operations and testing techniques and the role of the US Army Test and Evaluation Command in test operations.

9-0 LIST OF SYMBOLS

n = total number of working circuits in redundant arrangement

P = probability of successful operation of a redundant system

= total probability of failure

P_U = probability of material strengths lower than material strength U

P_V = probability of applied load lying between applied load V and $(V + dV)$

dP_c = incremental probability of failure

p = probability of one redundant logic unit working

$p(U)$ = probability density as a function of material strength U

$p(V)$ = probability density as a function of applied load V

$Q_i = (1 - R_i)$ = probability of failure of ith component or circuit

q = probability that voter is working correctly

R_c = reliability of each circuit

R_i = probability of success of ith component or circuit

R_{out} = system output reliability

R_s = system reliability

U = material strength

V = applied load

x = number of circuits operating that will enable redundant arrangement to function

9-1 INTRODUCTION

Similar pieces of equipment designed by different engineers can be either safe or hazardous. This occurs not only because of the varying capabilities of the engineers to recognize the hazards and incorporate measures to control them but also because of the varying effectiveness of the different types of controls employed. This chapter presents different methods of eliminating and controlling hazards that could lead to accidents and different methods of limiting the injuries and damages that could result should an accident occur. The methods are presented in rough order by priority of effectiveness. At the top of the list is designing the equipment to be intrinsically safe against specific hazards and thus to avoid accidents. At the bottom of the list is dependence on persons to read warning labels and to act safely. Safety is relative, and the use of these control measures is one of the factors that makes it so. In some cases, a high-priority method is impractical, and a method of lower priority must be used. It then becomes a designer's choice. This chapter identifies the available choices.

In designing for safety, numerous methods can be used to eliminate or control hazards. Some of these methods are more effective than others. For example, a barrier, such as a guard, over a piece of rotating equipment is much safer than a warning sign. MIL-STD-882 (Ref. 1), par. 4.3, lists many of these methods, and par. 4.4 specifies the order of precedence to be followed for using these methods to satisfy system safety requirements and to resolve identified hazards. This order of precedence may be briefly paraphrased as follows:

1. Use design to eliminate or control hazards.
2. Use protective safety devices where control by design is infeasible.
3. Use warning devices where neither design nor safety devices are practical.
4. Use procedures and training when the hazard cannot be eliminated through design, safety devices, or warning devices.

9-1.1 METHODS OF CONTROL

The methods used for eliminating and controlling hazards and for reducing their effects should an accident occur are described in par. 9-2. Key word descriptions of these methods are given in Table 9-1. The list shown in Table 9-1 roughly follows the order of precedence for

TABLE 9-1
HAZARD CONTROL METHODS

1. Control Energy Concepts (see par. 9-2.1)
2. Intrinsic Safety (see par. 9-2.2)
3. Isolation (see par. 9-2.3)
4. Lockouts, Lockins, and Interlocks (see par. 9-2.4)
5. Fail-Safe Designs (see par. 9-2.5)
6. Failure Minimization (see par. 9-2.6)
7. Safety Factors (see par. 9-2.7)
8. Warning Devices (see par. 9-2.8)
9. Labeling (see par. 9-2.9)
10. Minimization and Containment of Injury and Damage (see par. 9-2.10)
11. Escape and Rescue (see par. 9-2.11)
12. Weak Links (see par. 9-2.12)
13. Safe Test Considerations (see par. 9-2.13)

corrective safety action set forth in MIL-STD-882 (Ref. 1).

Although it is highly desirable to select the hazard control method with the lowest number, other considerations may make another method more practical. This is illustrated in Table 9-2, which uses the example of an electric hand drill. Persons have been killed by an electric shock when using metal-encased drills. (Tool manufacturers contend that the fatalities were due to improper repairs that resulted in a live conductor touching the metal case when the drill was used.) Other potentially fatal conditions could exist (1) if an encased tool bit drills into a live conductor or (2) if an operator drops a drill using 110-V power into a container of water or other conductive liquid and reaches in to retrieve it.

Table 9-2 indicates why and how safety tradeoffs must sometimes be made. For example, using a hand-cranked drill may be intrinsically safe, but it is ineffective for many uses. An air-powered drill would eliminate the possibility of electric shock, but it has its own lesser hazards and other adverse features—such as the unavailability of compressed air. Although the cordless battery drill is safe against electric shock, it requires periodic recharging of the battery, which has a limited life.

Thus, in practice, the hazard control method of highest priority, as established in Table 9-1, may not be practical in every case. However, as a general guide, priority should be given to designs that minimize unsafe conditions in order to minimize the need for procedural safeguards, i.e., actions on the part of the operator.

Many design engineers are unaware of the desired order of precedence for selecting methods to control hazards. In fact, a review of engineering literature, specifications, and standards reveals that many designers do not have a knowledge of safety principles and methods. Such words as "fail-safe" (Refs. 2 and 3), "foolproof" (Ref. 4), and even "perfectly safe" are requirements frequently seen and used synonymously even though the meanings are different. A fail-safe design allows for the failure of parts that may interrupt the normal operation

of the system, but the failed state of the system is such that no injury or damage will occur.

Many designers believe that to make a product "fail-safe" is the ultimate in accident-preventive design; unfortunately, not only do many of the designers not understand exactly what a fail-safe design is, they also do not know that certain other accident-preventive measures may be far superior. It is said that a product cannot be made "foolproof" because fools are so smart. Furthermore, since safety is a relative condition, a "perfectly safe" product is probably unachievable. Thus the safety engineer's job is partly educational, i.e., to provide inexperienced designers with some background in system safety, and partly identification of specific hazards in the proposed system design and recommendation of specific methods to control them.

9-1.2 ACCEPTABLE CONDITIONS (Ref. 5)

As the result of many years of experience, system safety engineers have developed general rules, principles, and priorities to make products safer. For example, to cite one principle, a safety engineer would be highly reluctant to accept a design in which one simple malfunction could result in serious injury or damage. The safety conditions that follow are considered generally acceptable for, and indicative of, good design. Analyses to determine the safety level of a system should take all of these conditions into consideration. The acceptable conditions include

1. The design requires at least two independent malfunctions, two independent errors, or a malfunction and an error that are independent of each other to occur before an accident will result. It is important that the functions or errors must be *independent* and that independence must be insured by analysis. An adjunct to this condition for extremely safety-critical* items that could cause a highly catastrophic accident requires more than two independent malfunctions or errors to occur before an accident will occur.
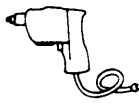
2. The design features for which analysis has indicated that an error would be safety critical will positively prevent an error in assembly, installation, connection, or operation. Examples are polarized connectors to prevent cross-connection of different circuits, asymmetrical fittings that cannot be assembled incorrectly, or check valves that cannot be reversed.

3. The design positively prevents a malfunction of one component or assembly from propagating other failures that could cause injury or damage. Such designs may be considered *fail-safe*. For example, a shear pin in a mechanical device that will fail when an excessive load that could cause damage to the equipment is applied.

4. The design will limit and control the operation, interaction, or sequence of functions in a system if such activities—unchecked—could allow an error or malfunction to cause an accident. For example, if an error in

---

*The term "safety critical" is used for any condition, part, or action that affects or could be affected by any safety aspect of a product.

TABLE 9-2. SAFETY MEASURE PRIORITIES (Ref. 5)

Type of Drill		Priority Number	Description of Safety Features	Other Advantages	Adverse Features
Mechanical Hand Drill		2	Intrinsic Safety Elimination of electricity use eliminates possibility of shock hazard.	Cost of drill is low.	Low mission effectiveness. Tiring to use. Must insure gears are guarded.
Cordless Battery Drill		2	Intrinsic Safety Uses electricity, but power level is too low to cause injurious shocks.	Can be used safely when operator is in water. Highly portable and convenient. No cord to be caught on projections. Can readily be taken into places with doors or other closed off places.	Limited power which limits size drill which can be used and type of material which can be drilled. Needs periodic recharging. Battery could explode.
Three-Wire Metal-Cased Drill		6	Failure Minimization Third wire provides path to ground for current if there is a short.	Cheap for manufacturers to change from 2-wire tool. Only connection on interior of metal case needed for third wire. No need to redesign and provide plastic case.	Path to ground may not be complete so will not be fail-safe. Trying to retrieve a live tool which has been dropped in water may result in a fatal shock.
Two-Wire Metal-Cased Drill		6	Failure Minimization More rugged design increases reliability so there will be fewer failures users will attempt to fix themselves.	Redesign not needed.	Manufacturer's contention that problem due to incorrect repairs may not be valid. Higher reliability means higher cost. Failures may still occur but at reduced rate. Cord flexing where it enters drill may expose live conductor. Dangerous in water.
Two-Wire Double-Insulated Drill		5	Fail-Safe Plastic protects user against shock if an internal short causes live conductor to contact case.	Two-wire cord slightly cheaper than three wire. Plastic case may be cheaper than metal.	Plastic not as abuse-resistant as metal. Cord flexing where it enters the case may expose live conductor. Dangerous in water.
Compressed Air Drill		2	Intrinsic Safety (electrically) Use of compressed air eliminates electricity and possibility of injurious shock.	More power and higher reliability than electric drills.	Very few homes and not all shops have compressed air (CA). Hazards and space requirements of compressed air systems make CA impracticable for the home. More expensive. Hose may make use inconvenient.

Willie Hammer, PRODUCT SAFETY MANAGEMENT AND ENGINEERING, © 1980, p. 110. Reproduced by permission of Prentice-Hall, Inc., Englewood Cliffs, NJ.

beginning operation B before beginning operation A could result in damage, an interlock to prevent B from being activated first would safely limit the operation.

5. The design will safely withstand an inadvertent release of energy higher than that normally required. For example, a regulating valve reduces the pressure of a gas in a supply cylinder to a lower level. The regulating valve could fail, and the full pressure in the supply cylinder imposed on what is normally a low-pressure line. To be acceptable, the low-pressure line should be able to withstand the inadvertent release of the high-pressure gas—either because of the strength of the piping itself or because of a relieving device incorporated into the line.

6. The design will positively prevent the buildup of energy to a level at which it could potentially cause an accident. For example, such buildup could be prevented

by means of relief valves, burst diaphragms, or fusible links.

These are the major conditions that will create confidence that the design is truly safe. When these conditions cannot be fully met, other conditions can be applied based on (1) visual and audible warnings and cautions and (2) isolation and containment. These conditions will also be discussed in subsequent paragraphs.

9-1.3 UNDESIRABLE CONDITIONS

The following conditions should be considered *undesirable* in any product unless the probability of an accident is extremely low:

1. The materiel has hazardous characteristics that can be eliminated or controlled by good design. This does not apply if the hazardous characteristic, e.g., radioactive, is necessitated by functional requirements or by characteristics of the product and if procedural safeguards are stipulated.

2. A single occurrence of personnel error or component malfunction could cause personnel injury or major damage to equipment or materiel.

9-2 HAZARD CONTROL METHODS (Ref. 5)

The methods—following the precedence in Table 9-1— for eliminating and controlling hazards and for reducing their effects should an accident occur are described in the paragraphs that follow.

9-2.1 THE ENERGY CONCEPT

The energy concept in safety matters is based on the principle that the magnitude of the effects of any mishap is a direct function of the amount of energy involved. In one sense, quantity-distance values for the storage of explosives are predicated on this idea, i.e., 100 kg of explosive will be more hazardous than 50 kg of the same explosive.

The same idea is inherent in the boiler and pressure vessel codes of the American Society of Mechanical Engineers (ASME). These codes contain more stringent safety requirements for equipment operating at pressures greater than 100 kPa (15 psi) than for equipment operating at less than 100 kPa (15 psi). Other codes have no safety requirements for pressure vessels with less than a given minimum volume—even though the pressure may be high—evidently because the total energy in the confined volume is not great.

Examples can be cited to show that the extent of injuries or damages will vary with the amount of uncontrolled energy being transferred or transformed. Damage in a collision between two vehicles will be directly proportional to the kinetic energy of impacting vehicles. The effects of a shock received from static electricity generated by wood, silk, or nylon—in contact with another triboelectric surface—will be far less than those from static electricity in the form of a lightning strike with its massive amount of energy.

In the context of the cited examples, the energy concept is undebatable. Unfortunately, the idea (sometimes put forth) that the safety level of any system is directly related to the amount of energy involved in the operation of that system is not. A high explosive may release the same amount of energy when it is initiated as a large quantity of gasoline does when it ignites, but in each case the ease with which the reaction is initiated and the effects that can be generated will differ significantly. Some explosives are very stable and must be initiated by less stable explosives.

The ignition of gasoline is far easier and, in this respect, its presence presents a far greater hazard than that of a stable high explosive. Once a reaction of a high explosive has been initiated, however, it cannot be interrupted. The shock wave and heat associated with the detonation can be devastating. On the other hand, the rate of transformation and release of energy is far slower with gasoline than it is with the explosive, and even inadvertent fires are controllable. In this respect, gasoline is less hazardous. Thus the amount of energy in a system is a very important safety consideration, but the type of energy is an equally important consideration.

Designers and analysts must be aware of these facts and give consideration to the damaging effects that can be generated by loss of control of an energy transfer or transformation process and to the means of preventing this loss of control. Ways to minimize the magnitudes of these adverse effects also must be considered. As pointed out in this paragraph, the uncontrolled release of energy is a highly significant event. An analyst making a preliminary hazard analysis should investigate first the hazard that can generate the most injuries or do the greatest damage; as a rule, this will occur where there can be an uncontrolled release of the largest amount of energy. This is also the area where maximal design effort to achieve a safe system will probably be concentrated.

9-2.2 INTRINSIC SAFETY

The most effective method of avoiding accidents is to create designs that are "intrinsically safe". Such designs are the closest thing to being "perfectly" safe. Intrinsic safety is achieved either by eliminating the hazard or by limiting the hazard to a level at which it can do no harm. Both of these methods are described more fully in pars. 9-2.2.1 and 9-2.2.2, respectively.

Most of the applications of the intrinsic safety principle are for electrical systems—although other applications are indicated in the paragraphs that follow—and it is from the electrical areas that Refs. 6 through 9 have been drawn. The requirements for intrinsically safe electrical systems—relative to the inadvertent ignition of flammable gases—are stated in Ref. 6 as

"2-1.1 Intrinsically safe apparatus and circuits shall meet two conditions:

"a. The energy available in the hazardous location shall be low enough under *normal* conditions so that it is incapable of igniting the specified hazardous atmospheric mixture due to arcing or temperature.

"b. The energy available in the hazardous location shall be low enough under *abnormal* conditions, i.e., with assumed fault conditions, so that it is incapable of igniting the specified hazardous atmospheric mixture due to arcing or temperature.".

National Fire Code No. 493 (Ref. 6) details how to insure that a system is intrinsically safe by testing it under the worst possible conditions—e.g., most ignitable mixture of gases that might be present, highest power input, and maximum voltage input. These intrinsic safety applications apply to electrical systems that have limited hazard levels.

The intrinsic safety of mechanical systems is more difficult to achieve since these systems generally contain parts in motion that can injure people and damage equipment and property. These accidents happen because of the kinetic energy available and the cutting, squeezing, or jabbing characteristics of the devices. By noting the extremely low energy levels just cited in pars. a and b for intrinsic safety in electrical circuits, it is easy to understand the difficulty in achieving comparable intrinsic safety in mechanical systems.

In an intrinsically safe system, even a human error will not result in an accident because the conditions do not exist whereby the accident can occur. It is important to note that a "fail-safe" system should not be considered an intrinsically safe system because conditions exist that could lead to an accident if the device making the arrangement "fail-safe" were to malfunction.

In mechanical systems, guards and barriers do not make a piece of equipment intrinsically safe. The hazardous condition exists; a person could remove the guard or barrier and be involved in an accident. Design techniques, however, are available for use where mechanical, intrinsic safety is required. Blades of fans or mixing devices can be made of very light materials that are frangible when striking objects such as fingers or other parts of the human body. Rotating or linear motion devices can be made with very low inertia so that the motion can be stopped with little effort. Low-energy power can be used where it will perform a required function and remain intrinsically safe. There are, of course, limitations to these techniques of design—such as when a functional requirement cannot be met with low power inputs.

9-2.2.1 Hazard Elimination

Hazards can sometimes be eliminated by careful design and selection of materials. Some common means are

1. Prevent cuts, scratches, or punctures of the skin by designing out rough edges, sharp corners, points, and the possibilities of jagged, broken surfaces.

2. Prevent fires by using nonflammable materials in items such as padding, hydraulic fluids, solvents, and electrical insulation.

3. Avoid electrical fires and excessive heat by using pneumatic or hydraulic systems instead of electric systems.

4. Avoid violent ruptures of pressure vessels that could generate shock waves by using hydraulic instead of pneumatic systems.

5. Eliminate leaks by using continuous one-piece lines instead of lines having many connectors.

6. Avoid injuries by eliminating protrusions such as handles and ornaments in vehicles which could cause injury during sudden stops.

9-2.2.2 Hazard-Level Limitation

It may not always be possible or practical to eliminate the hazard entirely; however, the level of the potential hazard can be limited so that no injuries or damage will result. For example, in the instances involving fatal electric shock from an electric drill (Table 9-2), it might have been possible to substitute low-voltage, low-amperage battery power that would not be injurious or damaging. The cordless battery drill is safe from electrical shock hazards. Note, however, that certain aspects of such a system may not be perfectly safe against other hazards, e.g., the battery could explode.

Designing for hazard-level limitation requires that designers determine

1. Which hazards could be present
2. The level at which each hazard would constitute a danger
3. The resulting limitations that should be specified
4. A means for automatically maintaining these limitations.

For example, a fuel gas such as methane is dangerous; it will burn—if an ignition source is present—when its concentration in the atmosphere reaches flammable limits. Therefore, it is common practice to insure that such an escaping fuel gas will never exceed 20% of the lower flammability limit. If the 20% point is ever exceeded, a blower could be automatically activated to reduce the flammable gas concentration, an inert gas could be automatically introduced, or a fire suppressant could be automatically injected.

Other examples of methods for reducing hazard levels follow:

1. Use sprays or other conductive coatings on a material to limit the amount of static electrical charge that can build up.

2. Use bleeder resistors on capacitors or capacitive circuits to reduce the electrical charge to acceptable levels after the power is shut off. The bleeder resistor should reduce the charge to acceptable levels in less time than it would take to gain access to the capacitor. Alternatively, when the cover of a capacitor circuit is removed, it could activate a capacitor-grounding relay.

3. Provide overflow arrangements that will prevent liquid levels from getting too high or from overflowing.

4. Use solid-state electrical devices where flammable or explosive gases may be present. Since mechanical devices are not required for switching operations, the potential for arcing with mechanical switches is eliminated.

9-2.3 ISOLATION

Isolation is the use of physical separation, guards, and barriers to isolate a recognized hazard from personnel and equipment to prevent or minimize hazards and to

control their effects. These methods and devices are some of the most commonly used safety measures. Barriers and guards are a more positive means of isolation than merely providing space between a hazardous device or operating equipment and the personnel who could be injured or equipment that could be damaged.

Isolation can be used to separate incompatible materials that together would constitute a hazard. Fire requires the presence of a fuel and an oxidizer in a flammable mixture, and it requires an ignition source. If any one of these elements is isolated from the others, the possibility of fire will be eliminated. Some highly flammable liquids are "blanketed" in their containers with nitrogen or another inert gas to isolate the liquids from contact with the oxygen in air.

Isolation is also used to limit the effects of uncontrolled energy release. Sensitive explosive materials are sometimes transported in special containers and handled in small quantities. The containers not only serve to contain the force of an explosion, should one occur, but they also isolate the devices from outside sources of energy that could cause activation of the devices. Tests to determine the amount of energy required to detonate or activate explosive or flammable materials can be conducted in isolation. A small amount of the material to be tested can be placed in a suitable container that will absorb or withstand the energy of the reaction.

Some materials, e.g., certain radioactive sources, are always harmful to humans and must always be isolated. If they constitute part of a normal process, continuous protection must be provided. Other examples of isolation protection required during scheduled operations include shielding persons from radiation generated by a welding arc, isolating workers in paint spraying booths, and having sandblasters wear totally enclosed suits. Isolation from mechanical devices that produce high levels of noise and vibration can be achieved by the use of vibration mounts, shields, or noise suppressors, or by locating the mechanical devices in a sound-isolated room or enclosure.

Machine guards and enclosures are widely used to isolate hazardous industrial equipment. These guards and enclosures are fixed over rotating parts, hot surfaces, pinch points, and electrical devices to prevent personnel from coming in contact with the hazard.

Other common examples of isolation using guards and barriers include

1. Placing extremely high-voltage components and circuits in a cage, vault, or fenced enclosure

2. Using thermal insulation between a heat source and the materials or components that could be adversely affected by the heat

3. Potting electrical connectors to isolate them from the deleterious effects of moisture and corrosives

4. Using stops to limit the motion of a mechanical device into an area where it will present a hazard to personnel or materiel

5. Using shields and screens to keep out foreign objects that could jam critical controls, orifices, or valves

6. Using shields on microwave ovens, X-ray equipment, and nuclear devices to contain emissions of harmful radiation

7. Using covered metal containers for oily rags to exclude air and to minimize the occurrence of spontaneous combustion

8. Using locked doors and panels to restrict access to internal working parts of moving machinery or high-voltage switching equipment.

9-2.4 LOCKOUTS, LOCKINS, AND INTERLOCKS

Lockouts, lockins, and interlocks are some of the most commonly used safety measures. Table 9-3 lists only a few of these devices and the measures that should be considered representative of the wide variety of types available. Their function is to prevent incompatible events from ever occurring, from occurring at the wrong time, or from occurring in the wrong sequence.

9-2.4.1 Lockouts and Lockins

The difference between a lockout and a lockin is relative. A lockout prevents an event from occurring or prevents some person, object, force, or factor from entering a dangerous zone. A lockin, on the other hand, maintains an event or condition, or keeps some person, object, force, or factor from leaving a safe, restricted zone. Locking a switch on an open circuit to prevent its being energized is a lockout; a similar lock on a live circuit to prevent current from being shut off is a lockin. Table 9-3 presents examples of lockouts and lockins.

Workers have been killed when the electrical or mechanical equipment they had deenergized for repair was inadvertently activated by other personnel. Workers repairing electrical circuits have been fatally shocked when the system was energized by someone who did not realize that it was under repair. A repairman working on a mechanical device such as a missile launcher or gun turret must also be protected against inadvertent activation of the mechanism. Accidents caused by the inadvertent actions of others can be avoided by use of lockouts. The switch that opens the activating circuit must be secured in place with a lock for which only the repairman or his immediate supervisor has the key or combination.

The use of blocks to immobilize equipment is another frequently used lockout. A common example is that of resting a raised vehicle on blocks of wood, steel, or stone to permit work on its underside. The blocks are more secure than some jacks that may fail or from which the vehicles may fall. Similarly, rocks or blocks of wood are wedged against the tires of a vehicle to prevent its rolling when a wheel is jacked up for replacement.

Other types of blocking devices used on vehicles as lockouts include the PARK position in an automatic transmission, which prevents motion until the driver is ready. The keyed ignition has several safety-related functions. In vehicles with automatic transmissions the key

TABLE 9-3. LOCKOUT AND LOCKIN DEVICES

Type	Mode of Operation
Ignition switch for aircraft and helicopters	When switch is off, the magnetos are grounded so no spark is produced if the engine is turned over.
Safing and arming devices in ammunition and missiles	Prevents explosive from being initiated until fired or launched and ammunition or missile is a safe distance from the launching device
Safety wiring and other locking devices on nuts and bolts	Prevents vibration from loosening fasteners
Locks securing electric switch levers	Prevents circuits from being energized inadvertently
Lockout to prevent filling tank cars with flammable liquid	Prevents pumping flammable fluid into tank car unless the system is adequately grounded
Blocks to prevent movement of vehicles	Prevents movement of vehicle along ground surface when vehicle has been jacked up
Parking blocks in vehicle transmissions	Prevents movement of vehicle along ground surface when powered wheels are on ground surface
Lockin device for electric power switch	Prevents shutting off power to essential equipment—e.g., safety-critical computer controller, safety exhaust fan, warning lights, emergency lights, and obstruction lights

lock prevents the PARK lockout from being removed inadvertently. In a vehicle with automatic transmission and power steering, the key lockout cannot prevent movement of the vehicle with the engine not running, but it does encourage the use of the engine by requiring that the ignition key be turned to unlock the PARK feature.

9-2.4.2 Interlocks

Interlocks are one of the most commonly used safety devices, especially with electrically operated equipment. They are provided to insure that an event does not occur

1. *Inadvertently*. To minimize the possibility of event B occurring inadvertently, an interlock is provided. It requires the operator to perform a preliminary, intentional action A before he can initiate event B. For example, before a critical switch may be thrown, the operator must first lift the cover that protects it.

2. *While a Hazardous Condition Exists*. An interlock may be placed on an access door of a cabinet containing high-voltage equipment. To make an adjustment, the door must be opened and the interlock now opens the circuit so that the unsafe condition no longer exists. For example, a short-range air defense system has a combination interlock and lockout arrangement to prevent missile firing until it is safe to do so. There is an electrical interlock on the overhead access hatch that will inhibit firing until the hatch is closed. Also, the commander has access to a lockout switch to prevent the gunner from firing the missile. When the commander is sure that conditions are safe, he unlocks the circuits to permit firing.

3. *Before the Event Is Scheduled*. Interlocks are desirable if the sequence of operations is important or necessary and a wrong sequence could cause a mishap. For example, an interlock may require that a cooling unit be turned on before a heat-producing system can be activated. Manufacturers provide numerous types of pushbutton switching arrangements that can function as interlocks. In each case an analysis of the operating procedures, and of the consequences resulting from a switching error, will indicate the type of switch to be used.

Interlocks take many forms. Table 9-4 indicates the operating principles of the types of interlocks most frequently used. In some cases it is possible to use any of several different principles in the design of one interlocking device. For example, an interlock to deactivate hazardous electrical equipment when panels or drawers are opened or removed for maintenance can be a limit switch, a tripping device, or a key interlock. Some interlocks themselves prevent action or motion; others send signals to other devices that prevent initiation of the action or motion. Many of the safeguards listed in Table 9-4 have interlocks that deactivate the equipment when the safeguard is bypassed. Other interlocks act to prevent an assembly or system from accidentally being put into an unsafe condition.

Sometimes a design requires that, for test purposes, a method of bypassing the safety interlock be provided. Therefore, interlocks can be of a type that can be bypassed manually after the cover or guard has been opened or other safeguards have been breached. Any interlocking device that can be bypassed for test purposes

TABLE 9-4. INTERLOCK DEVICES (Ref. 5)

Type	Mode of Operation
Limit switches, including: • Snap-acting switches • Positive-drive switches • Proximity switches	A wide variety of limit switches can be used for interlock purposes. In some cases the limit switch itself will open or close the circuit of which it forms a part; in others, a signal or lack of one from the limit switch will open or close a relay, which, in turn, will open or close a power circuit.
Tripping devices	Action releases a mechanical block or triggering device that either permits or stops motion.
Key interlock	Inserting and turning a key in a mechanical lock permits action.
Signal coding	Specifically coded sequences of pulses emitted by a transmitter must match the sequence in a suitable receiver. When the sequences match, the receiver initiates or permits action.
Motion interlock	Motion of the mechanism being guarded against prevents a guard or other access from being opened.
Parameter sensing	Presence, absence, excess, or inadequacy of pressure, temperature, flow, or other parameters permits or stops action.
Position interlock	Nonalignment of two or more parts prevents further action.
Two-hand controls	Two simultaneous physical actions by a person are required, sometimes within a specific length of time.
Sequential controls	Actions must be performed in the proper sequence, or operation is inhibited.
Timers and time delays	Operation of the equipment can take place only after a specific length of time has passed.
Path separation	Removal of a piece of the circuit or of the mechanical path physically prevents operation.
Photoelectric devices	Interruption or presence of light on a photoelectrical cell generates a signal that can stop or initiate action.
Magnetic or electromagnetic sensing	Presence of a magnetic material stops or initiates operation of the equipment.
Radio-frequency inductive	Sensing of any conductive material, especially steel or aluminum, causes it to operate.
Ultrasonics	Senses the presence of nonporous materials as that material moves into its control area and activates some event circuit.
Mercury switches	Mercury provides the path between two metal contacts through which current passes. The path can be broken by tilting the switch in which the mercury and contacts are sealed so that the mercury flows away from one contact and breaks the path for the current.

should be one that returns the safeguard to its operating position when the manual bypass has been removed. For example, closing the access door must automatically reset the interlock. As a positive measure, it is advisable to provide an indicator such as a light to warn that the bypass has been violated and the hazard is present—e.g., voltage present with no isolation barrier to prevent finger contact.

9-2.5 FAIL-SAFE DESIGNS

Fail-safe design insures that a failure will leave the system unaffected or functioning in a mode that cannot result in injury or damage. In most applications this design will cause inactivation of the system. In any case, the fundamental principle is that a fail-safe design will give first priority to protecting personnel, second priority to protecting the environment from catastrophic events such as explosions or fire, third priority to preventing damage to equipment, and fourth priority to preventing degraded operation or loss of function. There are three categories of fail-safe designs:

1. *Fail-Safe Passive Design (or "Fail-Passive" Design)*. This design inactivates the system and reduces it to its lowest energy level. The system will not operate until corrective action is taken and no further damage will result from the hazard causing the inactivation. Circuit breakers and fuses for protection of electrical circuits and equipment are fail-passive devices. The circuit breaker or fuse opens when the system reaches a dangerous level or a short circuit occurs; the system is then deenergized and safe.

2. *Fail-Safe Active Design (or "Fail-Active" Design)*. The fail-active design maintains an energized condition that keeps the system in a safe mode until corrective or overriding action occurs or until an alternate system is activated to eliminate the possibility of an accident. Redundancy created by the use of standby equipment is usually a part of the fail-active design. A fail-active design is incorporated in traffic signals. In most of its failure modes the signal will fail-active, i.e., switch to a flashing red-light mode that will control traffic in a way that should avoid accidents.

3. *Fail-Safe Operational Design (or "Fail-Operational" Design)*. This design allows the system to continue functioning safely until corrective action is possible; it is the most preferable of the fail-safe designs. Fig. 9-1 shows such a fail-safe operational orientation of feedwater valves for boilers. As indicated in Fig. 9-1(A), if the valve disk separates from the stem on which it is mounted, the water flow *over* the disk will force the valve closed and the boiler may be starved for water. When water flow is *under* the disk as indicated in Fig. 9-1(B), the water pressure will force the separated disk away from the seat and flow will continue (Ref. 5).

Fig. 9-2 illustrates two tanks in which the principal hazard is overpressurization. Each tank, therefore, is provided with a relief valve, sensor, and control to decouple the energy input when the sensing unit determines that a preset pressure level has been reached. In Fig. 9-2(A) the safe condition is with the relay in the open position, i.e.,

the motor stopped. The relay in the closed position—receiving a signal from the sensing unit that the pressure is within preset limits—will allow the compressor to operate. In Fig. 9-2(B) the safe condition is the gas valve in the closed position. Therefore, the gas valve should be of the type that is normally closed but is held in the open position only on the receipt of a signal from the sensing unit that the temperature (pressure) is within preset limits. When the limit is exceeded or there is a circuit failure, the gas valve will close (Ref. 5). Note that the valve in Fig. 9-1(B) and the relay in Fig. 9-2(A) must fail-safe in the open position; in Fig. 9-2(B) the gas valve must fail-safe in the closed position. These illustrations emphasize that, to be made fail-safe, each design must be analyzed for its own unique characteristics.

One fail-safe principle is predicated on the idea that only gravity is dependable in an emergency, e.g., semaphore switch signals on railways are weight-operated (gravity) devices. If the signal has an electrical failure, the heavy semaphore arm drops and activates a warning. The optimum designs of retractable landing gear for aircraft will drop and lock the wheels in the landing position if there is a failure in the hydraulic system that raises and lowers the gear.

The following examples further identify fail-safe devices:

1. The fuzes in Army artillery rounds provide a fail-safe feature that prevents detonation of the warhead if a short round fails to propel the warhead beyond the minimum safe distance from the firing position.

2. The air brakes on Army trucks, large trailers, and switch engines will activate to stop the vehicle if the air hose breaks or separates.

3. Motor controls for Army cranes and deadman throttles on Army locomotives and other vehicles and equipment will automatically shut down the electric motor or engine if the controls are released by the operator for any reason.

4. A mechanical safety interlock prevents large caliber guns from being fired if the gunner has failed to lock the breechblock.

Fail-safe systems are not to be regarded as the panacea for all safety problems because their operation generally depends on mechanical and electrical actions that might or might not occur. For example, snow and ice could jam the gravity semaphore switch signal used by the railroads to the extent that the weighted devices will not operate. An electrical fuse might not respond fast enough to prevent damage to a motor before the fuse blows. In addition, fuses and circuit breakers are not fail-safe with respect to protecting people against shock; the voltage and current levels at which they operate are far too high for personnel safety.

The term "fail-safe" is sometimes erroneously applied to redundant designs containing two or more items of the same equipment functioning simultaneously. The theory is that if one item fails, a second—and perhaps a third—item is available to keep the system operating. However, an accident can result if all of the redundant items fail. Ref. 5 cites an example: "On January 18, 1969, a three-engine airliner crashed into the ocean off Los Angeles,
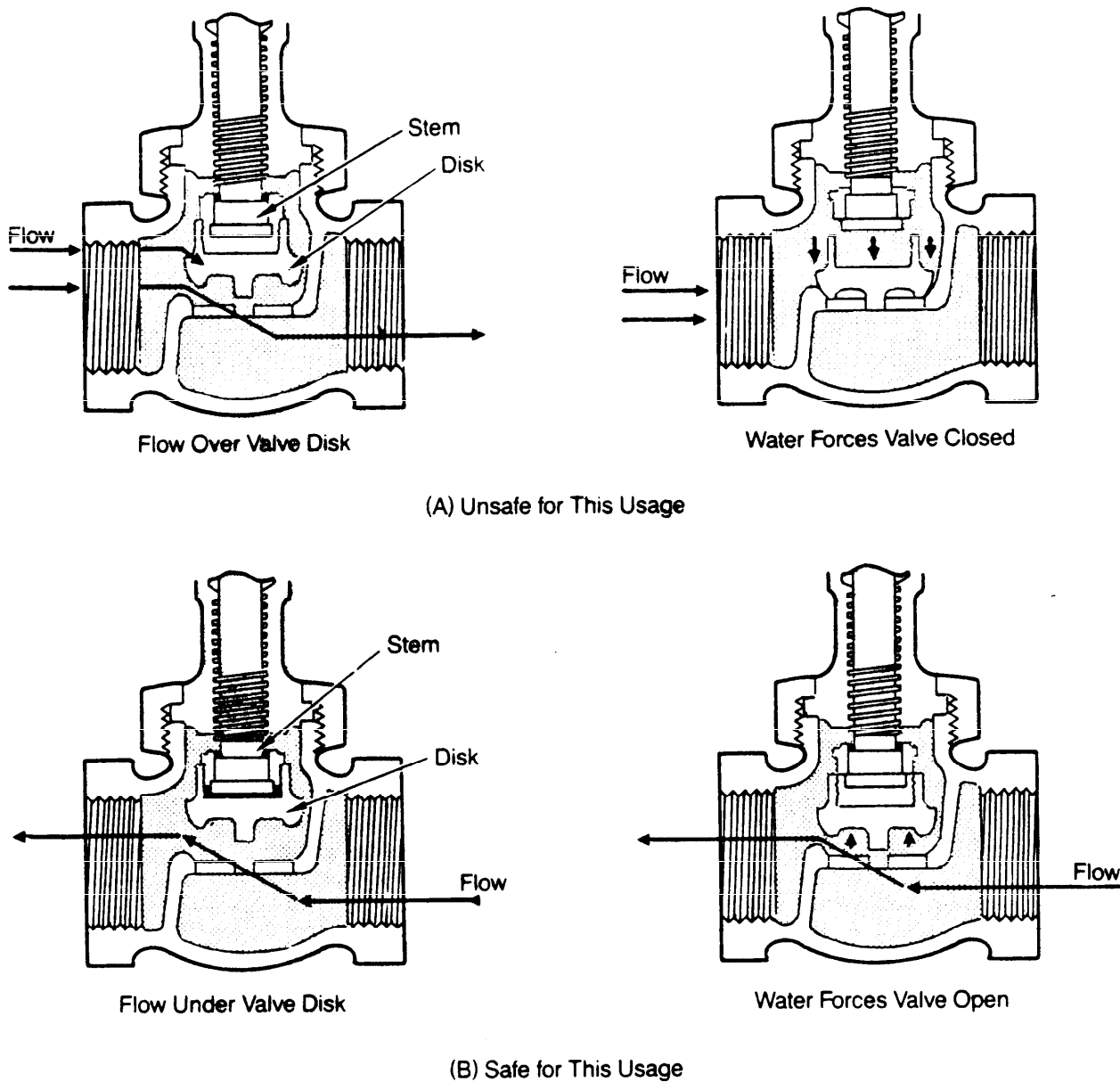
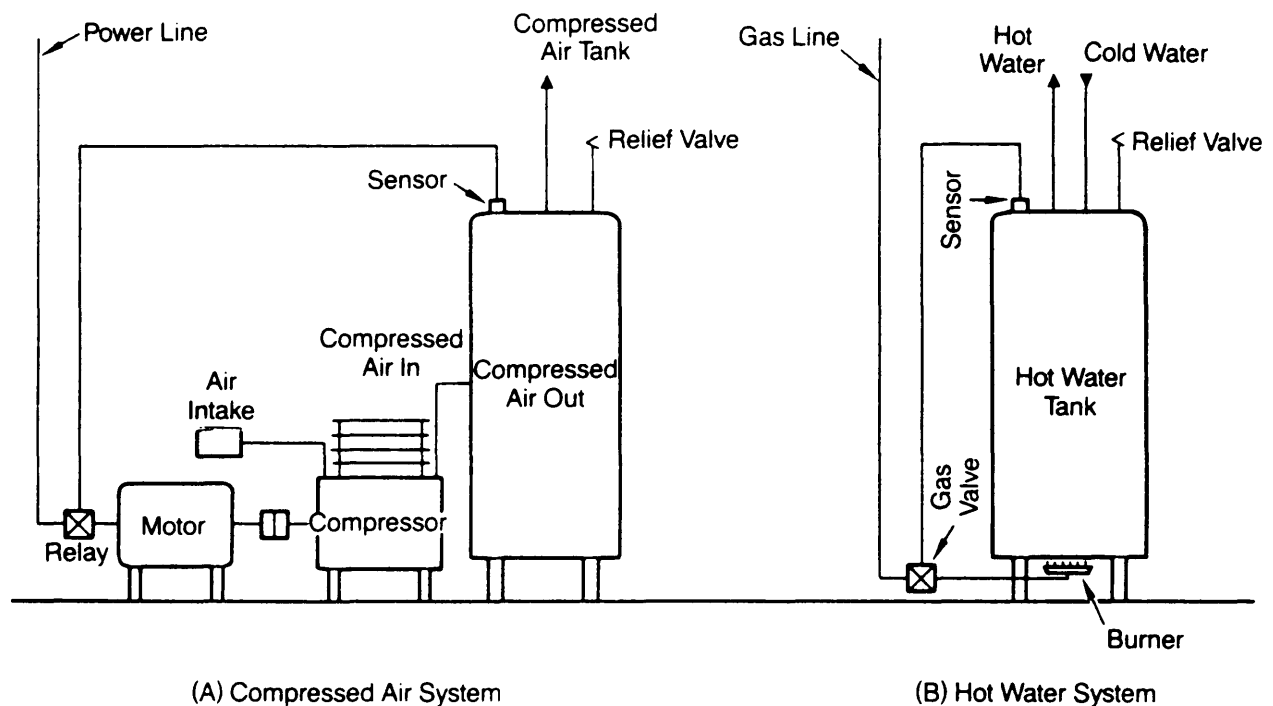**Figure 9-1. Fail-Safe Operational Design (Ref. 5)**

Willie Hammer, PRODUCT SAFETY MANAGEMENT AND ENGINEERING, © 1980, p. 116. Reproduced by permission of Prentice-Hall, Inc., Englewood Cliffs, NJ.

killing everyone aboard. The Federal Aviation Agency indicated that the accident could have been caused by a complete loss of electrical power. Although each engine drove a generator, one generator had been inoperative before takeoff. The pilot reported a fire in a second engine just before the crash and probably shut that engine and its generator down. As a result, the third and last generator may have overloaded and failed, cutting off all power." Redundant designs—as opposed to fail-safe designs—may reduce the possibility of a complete operational failure. In a properly designed fail-safe system, however, no accident should ever occur as a result of an operational failure.

9-2.6 FAILURE MINIMIZATION

Although fail-safe designs can sometimes be provided so that failures will not result in accidents, such designs are not always the most preferred goal. A fail-safe design may frequently shut down a system, process, or operation so critical that the fail-safe arrangement is less preferable than a process or operation that will fail only very rarely.

Figure 9-2. Establishing Fail-Safe Condition (Ref. 5)

For those situations in which a fail-safe design is infeasible, failure minimization can be the design goal. To minimize equipment failures and human errors that can cause accidents, the following five principal methods—failure rate reduction, monitoring, backout and recovery, safety factors and/or safety margins, and warnings—are employed:

1. *Failure Rate Reduction.* This is the principle upon which reliability engineering is predicated. It endeavors to use highly reliable components and designs—so that the overall system will have an expected use life beyond the proposed period of use—to reduce thereby the probability of failure during operation. Although its purpose is to reduce *all* malfunctions, the use of a reliability-engineered design has a favorable effect on strictly safety-related malfunctions, i.e., those that can result in injury or damage. Another technique in the failure rate reduction process is the planned replacement of parts so that their in-service time is always less than the estimated time before failure.

2. *Monitoring.* In this technique a critical parameter—such as temperature, noise, toxic gas concentration, vibration, pressure, or radiation—is kept under constant surveillance to insure that it remains within specified limits. If it exhibits an abnormal characteristic, corrective action can be taken promptly.

3. *Backout and Recovery.* This technique focuses upon contingencies. When a malfunction, error, or other adverse condition has developed into a dangerous situation that has not yet resulted in injury or damage, corrective actions are taken to limit deterioration of the situation. These corrective actions prevent certain injury, death, or equipment damage.

4. *Safety Factors and Margins.* Under this concept individual components are designed with strengths greater than those normally required to allow for variations in both strengths and stresses, unforeseen transients, material degradation, and other random factors. This is a form of failure rate reduction.

5. *Warnings.* Most types of warnings are means to apprise personnel of hazards, equipment problems, or other noteworthy conditions so they will not make incorrect decisions that could cause accidents.

Failure rate reduction, monitoring, and backout and recovery are discussed in pars. 9-2.6.1 through 9-2.6.3, respectively. Safety factors and margins are discussed in par. 9-2.7. Warnings and labeling are discussed in pars. 9-2.8 and 9-2.9, respectively.

9-2.6.1 Failure Rate Reduction

Failure rate reduction is a concept employed in reliability engineering to extend the expected lifetimes, or times between failure, of components and entire systems. In applying this concept there is an overlap between reliability and safety. Reliability is concerned with all malfunctions; safety is concerned with only those malfunctions that can result in injury or damage. Failure rates for parts

are considered to follow a time-in-service pattern similar to that shown in Fig. 9-3. Reliability engineers use a variety of methods to minimize the problems of component failures and, thereby, of system failures. Some of these methods are discussed in the paragraphs that follow. (For further details and applications concerning reliability, consult Refs. 10 through 13.)

Incorporating safety factors into equipment and structures was one of the first methods used to reduce failure rates. To create a safety factor, the engineer may design the product to be three, four, or five times as strong as required by his original calculations in order for it to withstand unanticipated transient loads and stresses and material degradation. (See par. 9-2.7.) Derating produces a similar result. Derating is applied to electronic equipment, other equipment that is stressed such as load-carrying structure, and wearout equipment such as engines. Wearout equipment wears and breaks at rates that are influenced by the operational rating of the equipment—how hard it will be used. One such rating is horsepower. The higher the horsepower output from a given engine, the greater the stress, the faster the wear, and a reduction in the assigned safety factor to prevent breakage or damage. Derating the equipment to operate at or below the rate that it is capable of sustaining, however, will increase the reliability of the component or equipment.

In addition to the use of safety factors or derating, the overall failure rates may be reduced by using various types of redundancies, using screening to remove failure-prone components, or replacing components before they wear out. If failures are safety-critical and would result in accidents, such reliability improvements will also decrease the number of accidents. These methods of reducing failure rates are described in the paragraphs that follow.

9-2.6.1.1 Derating

For electronic and wearout equipment, derating is the equivalent of safety factors for structures and certain types of mechanical equipment. To derate a piece of equipment, the first step is to determine its parts failure rating by test or experience. Parts will fail after specified intervals of service under specific conditions and stresses. Minimizing the adverse conditions that shorten the use life of a component will reduce its failure rate. One of the principal life-degrading conditions that affect electronic equipment is high temperature. In one method of derating, cooling is provided to reduce the operating temperature to the lowest practical level while the components are operating at their designed capacities. The effect of temperature on capacitors is shown in Fig. 9-4.

Fig. 9-4 also shows that a second degrading factor is the electrical stress factor, i.e., the ratio of operating stress to rated stress as measured by voltage. As the stress factor decreases, the failure rate also decreases. Therefore, derating can also be accomplished by using components whose stress capacity is much greater than that actually required, which reduces the stress ratio. If components with greater stress capacities are unavailable, too costly, or too bulky, it may be possible to achieve the same result through redundant arrangements.

9-2.6.1.2 Redundancy

The reduction in failure rates obtainable by derating is generally far less than can be obtained through redundancy. There are a number of categories of redundancy in common use—i.e., parallel, decision, standby, and series redundancy. Each is discussed in the paragraphs that follow.

9-2.6.1.2.1 Parallel Redundancy

In parallel redundant designs, the same functions are performed by two or more components, circuits, or subassemblies at the same time even though the combined outputs are not all required. In this arrangement, if one unit fails, the remaining units can still carry on the function of the system. This type of redundancy is generally
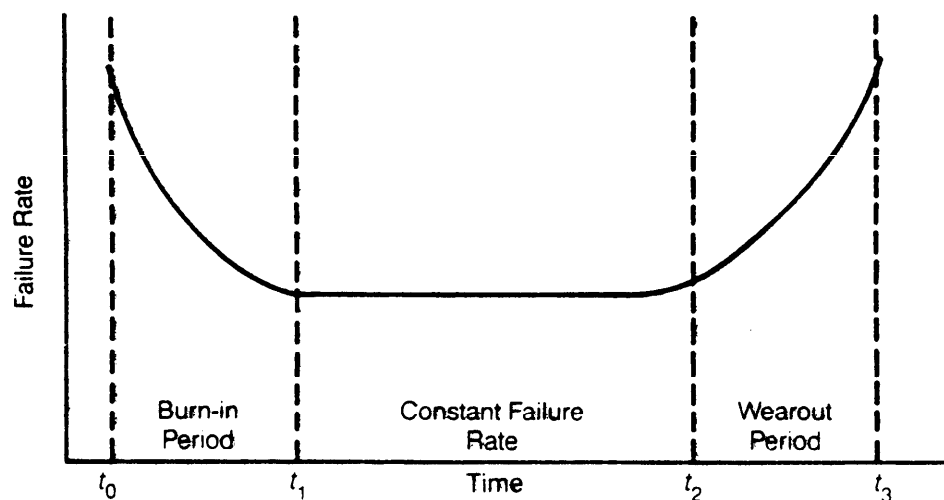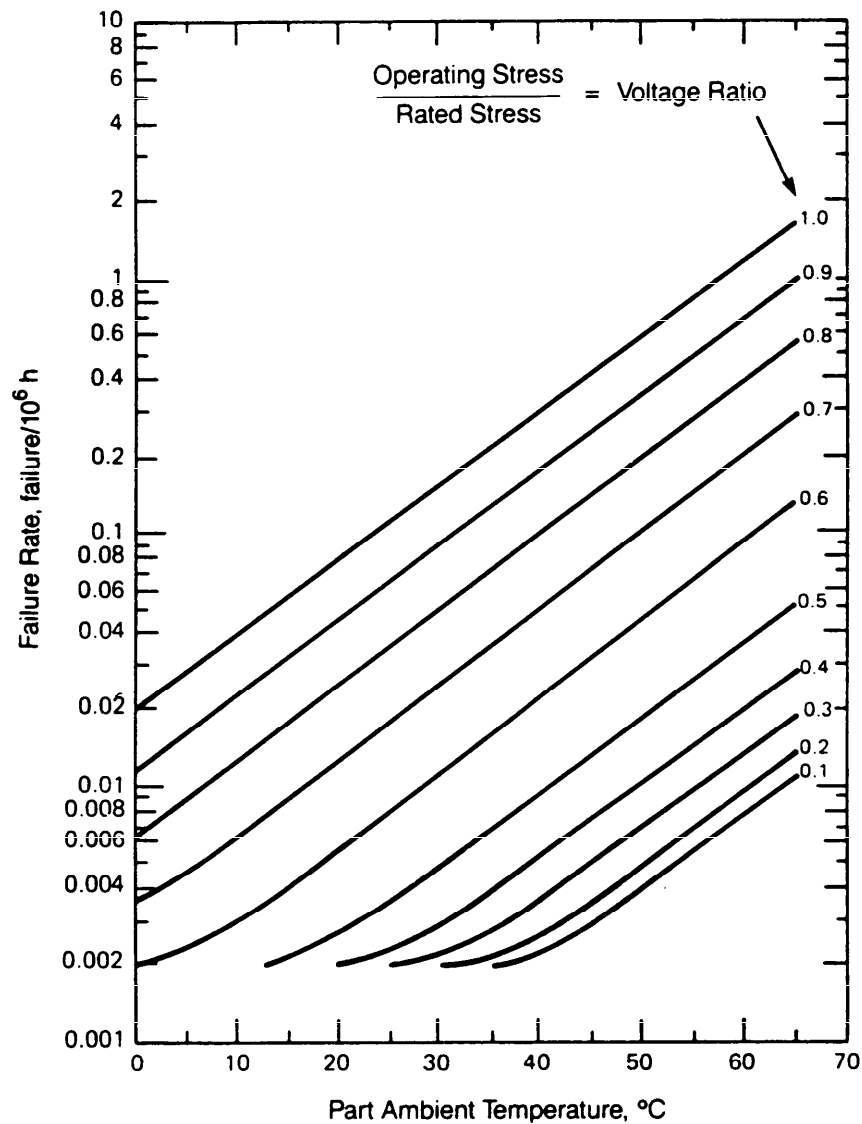

Figure 9-3.   Bathtub Curve

Figure 9-4.   Failure Rates for Polystyrene Capacitors (Ref. 5)

Willie Hammer, PRODUCT SAFETY MANAGEMENT AND ENGINEERING, © 1980, p. 72. Reproduced by permission of Prentice-Hall, Inc., Englewood Cliffs, NJ.

applied to equipment in continuous operation.

Parallel redundancy is also called replication. In the most common designs involving replication, there are generally only two components, circuits, or subassemblies in parallel, each of which could carry the entire load. An example is the replication of single components in parallel Circuits 1 and 2 in Fig. 9-5. Clearly, in this case there will be a successful output if Circuit 1, Circuit 2, or both Circuit 1 and Circuit 2 operate. Accordingly, the reliability of the parallel system may be determined by subtracting from unity the chance that both circuits will fail. Since Circuits 1 and 2 are independent, the parallel system output reliability R_{out} is

$$R_{out} = 1 - Q_1 Q_2 = 1 - (1 - R_1)(1 - R_2) \quad (9\text{-}1)$$

where

Q_1 = probability of failure of Circuit 1
Q_2 = probability of failure of Circuit 2
R_1 = probability of success of Circuit 1
R_2 = probability of success of Circuit 2.

If $R_1 = R_2 = 0.90$, the probability that there will be a successful output, given an input, is

$$R_{out} = 1 - (1 - 0.90)(1 - 0.90) = 0.99.$$

The idea of a redundant configuration can be extended to any number of k-parallel circuits as illustrated in Fig. 9-6—the design will operate when only one, two, or all k
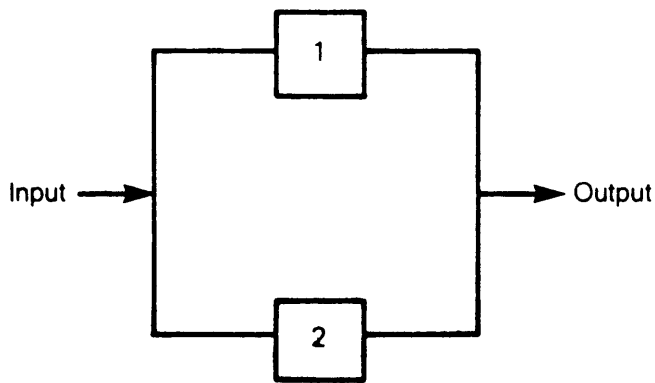
Figure 9-5.   Single Parallel Redundancy

Figure 9-6.   k-Parallel Redundancy

of the parallel circuits operate. The reliability of this k-redundant parallel system is

$$R_{out} = 1 - \prod_{i=1}^{i=k} (1 - R_i) \qquad (9\text{-}2)$$

where

R_i = reliability of the ith circuit.

In a double parallel redundancy mode, $k = 3$, an additional level of redundancy is added and R_{out}—assuming $R_1 = R_2 = R_3 = 0.90$—is

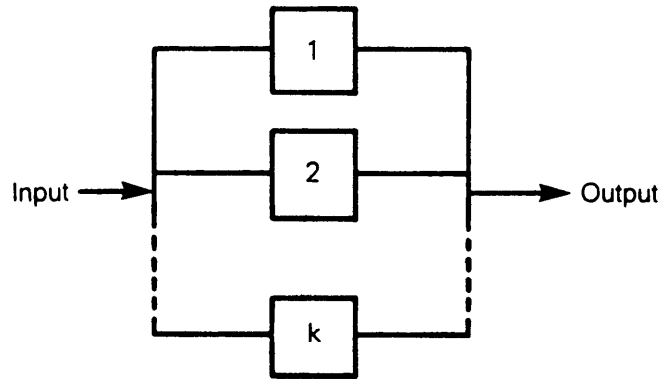$$R_{out} = 1 - (1 - 0.90)(1 - 0.90)(1 - 0.90) = 0.999.$$

When two or three circuits are in parallel redundancy, their normal operation is a load-sharing mode that, in effect, derates each individual circuit. Therefore, each component will have a longer life than if it operated with no redundancy. If one circuit in a double redundancy arrangement does fail, the other circuit has the capacity to assume the entire load until repairs can be made. The most commonly used design technique provides for successful operation with only one operating unit.

The system reliability R_s of a triple redundant arrangement in which at least two circuits must operate for the unit to provide the required output can be expressed by the statement

$$R_s = P(\text{at least 2 circuits operating})$$
$$= P(2 \text{ circuits working})$$
$$+ P(3 \text{ circuits working})$$

or in the mathematical terms for the general case—i.e., $R_1 \neq R_2 \neq R_3$—

$$R_s = R_1 R_2 Q_3 + R_1 R_3 Q_2 + R_2 R_3 Q_1 + R_1 R_2 R_3$$
$$= R_1 R_2 (1 - R_3) + R_1 R_3 (1 - R_2)$$
$$+ R_2 R_3 (1 - R_1) + R_1 R_2 R_3 \qquad (9\text{-}3)$$

where

P = probability of successful operation of a redundant system
R_i = reliability of ith circuit
$Q_i = (1 - R_i)$.

If the reliability R_c of each circuit is the same—i.e., $R_1 = R_2 = R_3$, Eq. 9-3 reduces to

$$R_s = 3R_c^2(1 + R_c) + R_c^3. \qquad (9\text{-}4)$$

Eq. 9-4 derives directly from the binomial probability expression

$$\begin{matrix} n \\ x \end{matrix} P^x (1 - P)^{n-x} \qquad (9\text{-}5)$$

where

n = total number of working circuits in redundant arrangement
x = number of circuits operating that will enable redundant arrangement to function.

Circuits involving more than triple redundancy are rare. The increase in reliability from more than three circuits is offset (1) by the increase in weight and (2) by the increase in probabilities of subsystem failure due to an increased number of components and, therefore, a requirement for increased maintenance. A notable exception is the Boeing 747 airliner, which has four redundant flight control systems.

9-2.6.1.2.2   Decision Redundancy

Some triple redundant circuits may use decision redundancy, whereby each circuit is monitored and one is selected for operation. An additional unit monitors the individual outputs and decides which one is to be used. The following paragraphs describe several techniques for deciding which circuit to use (Ref. 14):

1. *Majority Vote*. With this circuit selection technique, the triple redundant logic circuits feed their output signals into the decision unit. When one of the signals

differs from the other two, the decision unit (voter) accepts the two similar signals as being correct. The probability of having two failures at the same time is possible, but remote. However, if this does happen, or the voter fails, an error will result. Methods have been suggested to minimize even this remote possibility by replication in the voters (Ref. 15). With only one voter present, the probability of successful operation P of the redundant system is

$$P = q[p^3 + 3p^2(1 - p)] = qp^2(3 - 2p) \quad (9\text{-}6)$$

where

q = probability that the voter is working correctly
p = probability of one nonredundant logic unit working.

In Eq. 9-6

p^3 = probability that all three logic units work
$3p^2(1 - p)$ = probability that two logic units work and one unit fails.

2. *Median Select*. In this circuit selection arrangement, the middle value of the three signal outputs is selected. Variations are comparatively small when all three channels are working properly; however, the design of the decision unit still permits discrimination and acceptance of the middle-valued signal. The unit will still function if one or two of the redundant circuit channels fail, even if the failures result in outputs with opposite values.

3. *Triple Redundancy Incorporating Self-Adaptive Failure Exclusion (TRISAFE)*. The output signals from three amplifiers are connected to a common voting point where feedback gain is provided to each amplifier. If one channel fails, the gain in one of the other amplifiers increases to compensate for the loss while the third amplifier continues to operate normally. The system will function unless all three output signals fail.

4. *Self-Organizing Concept (SOC)*. This circuit selection technique involves the use of the same circuit whenever it is functioning correctly. In the event of a failure, an alternate signal path is selected. (This is analogous to the functioning of the human nervous system.) A detection unit determines when a failure has occurred and switches to an alternate circuit until the output of the preferred circuit has been corrected.

9-2.6.1.2.3 Standby System Redundancy

Another method of increasing product reliability through redundancy is to provide inoperative or idling standby units, as shown in Fig. 9-7, that take over when and if an operating unit fails. Failure detection and switchover devices to activate the standby unit at the proper time must be present in the system. Because the operating unit logically would wear out much more rapidly than the inoperative or idling redundant unit would, the operating unit should require replacement much more frequently. For this reason, the operations of the units are occasionally alternated. In some cases, one unit can provide standby capacity for several operating units.

Activation of the standby unit may be manual, automatic, or both. A common example is the infrared remote control system on a TV set—if the infrared system fails, channel selection can be done manually. When selecting channels manually, the viewer is the detecting and activating agency. In other usages, the failure of the operating unit could be detected by a monitoring unit and indicated to the operator so that he or she can activate the standby system if and when he or she wants. In fully automatic systems, detection and activation are interlocked so that failure of the operating unit causes activation of the standby equipment with minimal delay.

Major Army communications installations and field hospitals frequently have a backup power source for subsystems critical to their missions. Diesel-powered generators may be standbys for commercial power. The criticality of the potential loss of power determines the type of backup to be used and whether switching should be manual or automatic.

The failure-detecting and system-switching devices do not have 100% reliability and may malfunction. Thus the standby units may fail to activate when required, or they
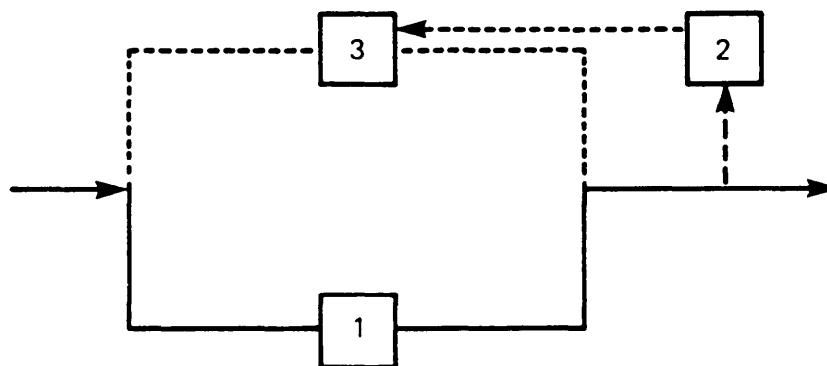

Figure 9-7. Standby System

may activate erroneously. Generally, erroneous activation is not a problem, but any such possibility should be investigated when the system is designed. In some instances, the standby units—especially those rarely used or tested—may fail. The possibility that the detection, switching, and standby units may themselves fail limits the reliability attainable by this method.

There are numerous ways to lay out standby systems. In the arrangement shown in Fig. 9-7, Component 1 will operate continuously until it fails. When Component 2 senses this, it will activate Component 3. The probability R_s that the system will provide an output, therefore, is dependent on the reliability of Component 1 and then on that of Components 2 and 3 when Component 1 fails. This probability is expressed as

$$R_s = R_1 + Q_1 R_2 R_3. \qquad (9\text{-}7)$$

If the reliability of each of the three components is 0.90,

$$R_s = 0.9 + 0.1(0.9)(0.9) = 0.981.$$

9-2.6.1.2.4 Series Redundancy

The series redundant arrangement consists of multiple units arranged in a series—wherein all units must operate before an output signal can be generated—as shown in Fig. 9-8. Generally, series redundancy is used to prevent inadvertent outputs that could be damaging if they occurred prematurely. In a series arrangement, all of the units must be switched from safe, open, or off states to activated states before they will release an output to energize a device downstream. With series redundancy, all units in the series must fail before the device can be activated inadvertently; therefore, the probability of failure is generally low.

A series such as that shown in Fig. 9-8 is frequently used to prevent an output unless 1, 2, and 3 fail simultaneously. In such cases they may be called "blocking elements". The probability that such an arrangement will work effectively is

$$\begin{aligned} R_s &= 1 - Q_1 Q_2 Q_3 \\ &= 1 - (1 - R_1)(1 - R_2)(1 - R_3). \quad (9\text{-}8) \end{aligned}$$

If each element has a reliability equal to 0.90,

$$R_s = 1 - 0.10(0.10)(0.10) = 0.999.$$

For the general redundant case in series

$$R_s = 1 - \prod_{i=1}^{i=k} (1 - R_i) \qquad (9\text{-}9)$$

where
  R_i = reliability of ith component.

9-2.6.1.3 Screening (Ref. 5)

Component failures can be reduced by imposing strict manufacturing practices and quality control techniques to narrow the dispersion of component characteristics which contribute to these component failures. Inferior components are rejected or are less likely to occur by these procedures. Screening eliminates those components that fail inspection tests, but it also attempts to eliminate components that pass inspection but give an indication that they will have a short operational life. Screening involves four steps, namely,

1. *Parameter Selection.* Parameters, whose limits are not to be exceeded by the component are selected. One such parameter may be operational use life.

2. *Parameter Limits.* The limit for each parameter is established. When product requirements are known, the limits can be based on expected operating conditions.

3. *Inspection and Testing.* The components are inspected and tested to verify that they meet the established limitations.

4. *Component Rejection.* Items that fail to meet any limit are rejected.

In one type of screening for reliability, both lower and upper limits may have to be observed. An example is an over- and undervoltage protection device. This device must activate to protect critical electrical equipment when the voltage regulator fails to keep the voltage within the acceptable limits, both high and low. Weak-link, burn-in, and accelerated-life screening are discussed in the paragraphs that follow.

9-2.6.1.3.1 Weak-Link Screening

Some mechanical designs use so-called "weak links" to restrain various loads of equipment or ammunition. This type of design feature is incorporated in an Army missile to hold the missile in position until the rocket motor is ignited. The mechanical device must be strong enough to secure the missile against all forces encountered when the tracked launch vehicle is in motion. The device must not be so strong, however, that it will restrain the missile when the rocket motor is activated.

Aircraft drag chutes use a similar weak link to attach the chute to the aircraft. If the chute is accidentally deployed during normal flight, the forces are great enough to break the link and thus prevent an accident.
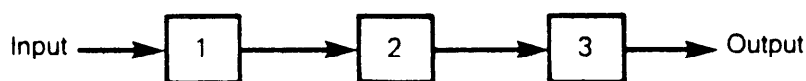

Input ⟶ 1 ⟶ 2 ⟶ 3 ⟶ Output

Figure 9-8.   Series Redundancy

When the chute is deployed after touchdown on the runway and the aircraft is moving much slower, the link holds to retain the chute and slows the aircraft. To set the lower and upper limits for such devices, careful calculation and testing are required.

Lower and upper limits are also required for such devices as safety pressure diaphragms. The diaphragms must not fail at less than the normal pressure plus an added increment for safety but must rupture at the maximum safe pressure level. Par. 9-2.12 contains a thorough discussion of weak links.

9-2.6.1.3.2 Burn-In Screening

Screening may also be done by operating the component or assembly under test for the time period during which burn-in failures may be expected to occur. It is seen, by referring to the bathtub curve in Fig. 9-3, that this type of screening would eliminate those items that would fail before the constant failure rate portion of the curve begins. Burn-in screening is based on the assumption that component defects caused by manufacturing or assembly errors will become apparent soon after the components begin operation. Thus, substandard components can be replaced at the factory and, thereby, reduce the users' maintenance burdens.

To develop a burn-in test program, the test engineer establishes the types, levels, and durations of stress that the components or assemblies must endure to insure that they are free of manufacturing defects. The objective is to select levels and durations of stress that will eliminate substandard items without damaging the satisfactory items. Immediately after the test the items are inspected visually for any other damage not detected by the test equipment.

9-2.6.1.3.3 Accelerated-Life Testing

Another type of screening is accelerated-life testing to determine quickly the life expectancy of a long-lived component by testing it to destruction with extremely high stresses over a short period of time. Such stresses are much higher than those expected to be encountered under normal operations. Accelerated-life testing differs from the other types of screening previously described in that it tests only a sample lot; obviously, it cannot be used as a 100% method of screening. Accelerated-life testing has other weaknesses. The principal one is that the testing may introduce artificial failure modes. For example, an increase in shock and vibration may cause connections to fail or break when such failures would not occur under the usual operating conditions. The processes whereby components normally wear out may be altered by the tests, i.e., produce unusual conditions resulting in many more failures than usual. There may also be difficulty in determining the true relationship between the relative increases in stress and the failure rate. Some types of stress may not be time dependent, so increasing the stress levels for short time periods may not accelerate the effects. Accordingly, test parameters must be selected and evaluated carefully to insure their suitability for accelerated testing.

There are three types of accelerated-life testing. In the basic type, constant-stress testing, several groups of components are stressed at the same constant level. The size and composition of each sample group are selected to permit the analyst to draw valid statistical conclusions and make reasonable decisions on the basis of the analysis.

The other two types of accelerated-life testing are step testing and progressive-stress testing. In step testing increasingly higher levels of stress are applied to the sample lots of components at specific time intervals. In progressive-type testing sample lots are started at different stress levels that are increased at a constant, regular rate.

9-2.6.1.4 Timed Replacements

To maintain a constant low failure rate, components should be replaced as part of a scheduled maintenance program before they wear out. In addition, some critical operations require that the frequency of failures be held to an absolute minimum. Consequently, the replacement of parts before they fail must be scheduled carefully. Replacement too soon is wasteful, creates an unnecessary maintenance and supply workload, and can result in increased failures due to maintenance errors.

Timed replacements can be scheduled in two principal ways. The more common method uses the manufacturer's failure data such as that shown in Table 9-5. The analyst estimates the average operating time for the system during one operational cycle, and he divides his time into the manufacturer's predicted use life for the component. The result is the number of operational cycles at which wearout failures may begin. The analyst then recommends that the component be replaced via scheduled maintenance before the use of the system exceeds the calculated number of operational cycles.

The second means of determining the optimum time to replace components in operating systems is by noting component degradation, or drift. Most components in electronic equipment deteriorate gradually. Under this method, an assembly undergoes a periodic series of tests for a specific operating characteristic such as current flow through a particular circuit with a specific voltage. The results are plotted, and the changes, or drift, are noted. The time at which the operating characteristic of the assembly approaches the failure point becomes the time at which the components involved will be replaced in operational systems.

A precise technique for measuring degradation of components to establish scheduled replacement times was developed for aircraft engines. This technique, known as the Spectrometric Oil Analysis Program (SOAP), involves the periodic measurement of minute amounts of aluminum, iron, copper, and other metals in engine oil to determine the amount of wear and to schedule engine overhauls. SOAP analyses can determine where abrasion is taking place and the rate at which the metal is abrading. From this information a maintenance schedule can then be established. The Army Oil Analysis Program (AOAP), described in AR 750-22 (Ref. 16), employs the SOAP principle to determine wear of aircraft and other systems.

TABLE 9-5
GENERIC FAILURE RATES (Ref. 5)*

Part	Failure Rate, failures/10^6h
Batteries, rechargeable	27.027
Bearings, general	21.921
Bearings, ball	9.142
Blowers and fans, centrifugal	9.542
Boards, printed circuits	0.003
Connections, solder	0.0039
Connections, welded	0.0017
Connections, wire wrap	0.000014
Connectors, rectangular	0.0065
Engines, diesel	1733.111
Engines, gas turbine	577.397
Gaskets and seals, gaskets	1.433
Gaskets and seals, O-rings	1.182
Gaskets and packing	0.24
Heater, electrical	2.151
Hoses, general	0.240
Instruments, meter	0.366
Instruments, indicator, air pressure	1.020
Instruments, indicator, fuel quantity	78.811
Instruments, indicator, liquid level	11.905
Instruments, indicator, temperature	62.016
Instruments, indicator, velocity	97.096
Mechanism, power transmission, coupling	4.662
Mechanism, power transmission, fan belt	4.007
Mechanism, power transmission, gear box	11.726
Mechanism, power transmission, pulley	39.279
Motors, electrical, inductor	14.774
Motors, electrical fract. hp, ac	7.552
Motors, electrical 2 hp, ac	2.413
Motors, electrical 5 hp, ac	4.825
Motors, electrical 10 hp, ac	1.206
Motors, electrical motor generator set	27.778
Generators	9.34
Generators, turbine driven	11.925
Pumps, boiler feed	0.422
Pumps, centrifugal	12.058
Pumps, fuel	23.121
Relays, general	0.166
Relays, latching	0.569
Switches, push-button	0.270
Switches, rotary	1.329
Tanks, fuel	7.745
Valves, check	3.014
Valves, globe	0.185
Valves, relief	1.514
Valves, solenoid	2.404

*Material for this table extracted from the *Nonelectronic Reliability Notebook*, RADC-TR-75-22, Rome Air Development Center, Griffis Air Force Base, NY, January 1975.

The SOAP technique is finding other applications for measuring equipment degradation.

Mechanical devices also can be used to signal the wearing out, or time replacement, of components. Examples are the wear-out bars on pneumatic tires and the chirping sound emitted by worn-out brake linings.

9-2.6.2 Monitoring

The use of monitoring as a method of minimizing failures involves keeping a selected parameter, such as temperature or pressure, under surveillance. The objective is to insure that these selected parameters do not reach dangerous levels that could lead to a contingency. Thus monitoring enables the avoidance of contingencies that could deteriorate quickly into disasters.

Monitors can be used to indicate
1. Whether or not the system or one of its subsystems or components is ready for operation or is operating satisfactorily as programmed
2. Whether or not the required input is being provided
3. Whether a desired or an undesired output is being generated
4. Whether or not a specific condition exists
5. Whether or not a specified limit is being exceeded
6. Whether or not the measured parameter is abnormal.

To be of value, a monitoring system must also include some provision for a tie-in with a warning system, an interlock, or another means of triggering corrective action. The warning system may convey information to an operator, who then takes corrective action. An interlock enables an out-of-limit signal to shut down the system. Another type of monitoring system may determine that a fire exists, activate a fire-suppressant system, and sound an alarm.

The monitoring process generally consists of the functions of detection, measurement, interpretation, and response. Each of these functions is discussed in the paragraphs that follow.

9-2.6.2.1 Detection

A monitor must be capable of sensing its specific parameter in spite of the presence of any other programmed or emergency environmental stress that may arise. It must be able to sense only that specific parameter and not be affected by similar but extraneous parameters. In some cases the sensing function may be variable—i.e., under the control of an operator to monitor continuously, continually but intermittently, or intermittently. The monitor must be capable of detecting the hazard at a level low enough to permit corrective action before emergency action is required. For example, a toxic gas detector must be capable of measuring extremely small concentrations of toxicants.

The sensor of the monitoring device also should be located where it can sense most quickly and accurately the parameter for which it has been selected. For example, fire detectors in Army tanks, personnel carriers, and other

mobile equipment must be located in the areas with the highest probability for fires, i.e., where fuel can spill near hot engine parts. Carbon monoxide detectors must be placed in areas where personnel could be exposed to leaking exhaust systems.

9-2.6.2.2 Measurement

Many types of monitoring devices exist. Two types of significance to safety are discussed. The first type senses only one of two conditions, such as ON or OFF. The second type of monitor compares existing and predetermined safe levels of the parameter. Methods for such monitoring vary from extremely simple to quite complex. An example of a simple method is a display, such as a dial, marked with the predetermined limit and an indicator that shows the existing level. An operator observes and compares the existing level with the limit to determine whether or not there is an abnormality. One style of gage that monitors engine oil pressure in an automobile is of this type.

9-2.6.2.3 Interpretation

The type of monitoring device designed to signal the operator is, in reality, providing a warning that corrective action must be taken to avoid a possible contingency. Therefore, operators must understand clearly the exact meanings of the information displayed by the monitor to make the appropriate decision regarding corrective action. Accordingly, the parameters selected for monitoring should be meaningful. The displays should provide timely and easily recognizable information, and—depending upon the individual requirements—the readouts should be displayed continuously, when preset limits are exceeded, or on demand.

9-2.6.2.4 Response

When a monitor indicates a normal situation, no response is necessary other than continuation of the operation. If corrective action is required, the more time available to the operator for interpreting the information, reaching a decision, and responding, the more likely that his or her decision and response will be proper and effective. Accordingly, the monitor should signal as early as possible the approach of an adverse condition. The level at which a monitor will indicate the existence of a problem can sometimes be set far in advance of the actual danger level—a desired characteristic. The proper warning level can be established by analyzing the situation to be monitored and the urgency of the contingency that could arise. For example, for personnel exposed to carbon monoxide (CO) over an 8-h day, the CO danger level is 35 parts per million (ppm). A CO monitor for an enclosed space might be set to trigger a signal when the CO concentration reached 30 ppm. At this point the atmosphere is still breathable, but the deficiency indicates a situation that should be investigated.

If the monitoring device requires response by a person, the system operation should be analyzed to insure that there will be adequate time to take corrective action under foreseeable circumstances. If an immediate corrective action were required to avert a serious, critical, or catastrophic condition, the monitor should be interlocked to activate automatically hazard suppression or damage-containment devices. Other features to be considered during the design of monitors and their attendant warning or activation devices are that

1. Monitors must function at the highest practical reliability levels. In extremely critical applications, they must be designed to indicate any failures of their own circuits or to permit periodic, quick checks of these circuits. Monitoring devices must be analyzed as thoroughly as the system they are to monitor because in the past false indications have induced personnel to take actions that have proved fatal. Monitoring and warning circuits should be analyzed by the same logic analysis methods used for other electrical and electronic networks. (See Chapter 5.)

2. Failure of monitoring equipment or circuits must not introduce other hazardous conditions or damaging effects into the system.

3. Monitoring systems must be easy to maintain, check, and calibrate. Procedures must be provided for these operations.

4. If system failure could cause the loss of power to the monitoring and warning circuits, it may be desirable to provide them with independent power sources and circuits.

5. The energy level for monitoring must not exceed that which would constitute or contribute to a hazard to the system being monitored.

6. Circuitry within the monitoring system must not provide a path that would cause degradation or failure of the system during operation. (See sneak circuit analysis in par. 5-6.) Monitoring circuit devices should not generate radio frequency (RF) energy or other noise in other circuits.

7. Power for monitoring should not be routed through system circuitry in a manner that could cause an unsafe condition, remove a blocking element, or cause inadvertent activation.

A few of the many applications of monitoring are

1. Temperature and pressure monitors for engines
2. Radiation monitors for nuclear sources
3. Odorants to indicate leakage of gases that may be toxic or highly flammable
4. Gas monitors to determine the presence of toxic or flammable substances
5. Analysis (SOAP) of engine oil to detect minute amounts of aluminum, iron, copper, and other metals by which wear can be determined
6. Signature analysis—also referred to as likelihood analysis—to identify wear by means of comparison of vibration patterns. A master pattern is recorded in the vibrations emitted by new equipment that is running satisfactorily. Subsequent recordings are made at intervals as the equipment ages. These patterns are compared with the master pattern to identify changes in the functioning of the equipment and to determine the criticality of the changes and whether or not the equipment should be repaired.

7. Infrared detectors in specific frequency bands to indicate the presence of hot spots or flames

8. Liquid level indicators to warn or initiate action when the liquid reaches a preset level or overflows.

9-2.6.3 Backout and Recovery

A malfunction, error, or other adverse condition may develop into an extremely dangerous contingency situation that has not yet resulted in any injury or damage. This is a critical period. With suitable corrective action an accident can be avoided; however, failure to act, or incorrect or inadequate actions, can permit the situation to deteriorate into a mishap. This critical interim period extends from the time the contingency begins to the time that either normalcy is restored or a full-scale mishap develops. If recovery takes place, the incident can be considered a near miss. Actions that should be taken in such a situation must be established by a contingency analysis for each particular operation. (See par. 8-3.) In general, these actions can be divided into

1. *Restoring Normal Sequence*. The conduct of certain operations in wrong sequences can subsequently lead to a failure and mishap. There may be an interval, however, during which the operator can correct the situation without damage simply by proceeding directly to the correct step that may have been bypassed or to another predetermined step at which a new start can be made.

2. *Aborting Entire Operation*. Each operation has a step(s) at which it can be halted without injury to personnel. Sometimes that halt can also be made without damage to equipment, but this is secondary to safeguarding personnel. The detection of a missing bolt, leaking oil line, or inoperative device before the operation begins might cause an abort whose only adverse effect would be delay. However, an abort after the operation begins could have effects of varying magnitudes.

3. *Inactivating Only Malfunctioning Equipment*. This action can be accomplished if the problem falls into one of the following categories:

    a. The equipment to be inactivated is never essential to the overall operation.

    b. Because of redundancy, inactivation of the equipment will not affect the operation of the system.

    c. The equipment to be inactivated has already fulfilled its function in the overall operation and is no longer required.

    d. A temporary substitution can be made for the equipment to be inactivated.

4. *Suppressing Hazard*. When a hazard becomes apparent or exceeds a specific limit, the hazard can sometimes be removed or suppressed. For example, spillage of a large amount of gasoline could produce a flammable mixture resulting in fire. However, the possibility of an accident is eliminated by flushing away the gasoline and recreating a normal atmosphere. Depending on the monitoring and control equipment available, hazard suppression may be automatic or manual.

9-2.7 SAFETY FACTORS

The use of safety factors to minimize failures of structures and materials is an ancient concept. The concept is simple, i.e., make the structure or material much stronger than the calculations indicate would normally be required to resist potential stresses. Safety factors are widely used today.

9-2.7.1 History and Uses of Safety Factors

Ref. 17 provides a history of the use of safety factors for aircraft structures. In 1900 Wilbur Wright stated that he was building and testing his machine "to sustain about five times my weight", or using a safety factor of 5. Later aircraft safety factors varied and then were standardized at 1.5. Conferences (for which the papers in Ref. 17 were written) were then held to determine whether the safety factor for transport aircraft structures should be reduced to 1.25.

The use of different safety factors indicates that the selection of the value is arbitrary; it represents a compromise among considerations of safety; weight; cost; and uncertainties of quality, loads, operating conditions, and other affecting factors. For example, passenger aircraft—in which many people could be killed in the event of a failure—may be designed with a safety factor of 1.5 or 1.25, but a pressure vessel—whose rupture could result in the injury to or deaths of a few persons—may be designed with a safety factor of 3, 4, or 5. This apparent inconsistency in safety factors may be partly explained by the differences in expected conditions of operation during the life of the equipment.

Aircraft are usually operated, maintained, and inspected by skilled and knowledgeable personnel who are required to stay current. In addition, the environment in which the aircraft will operate is known with some degree of confidence. Also a large aircraft with a safety factor of 5 would be difficult to get off the ground because of its increased weight and uneconomical to operate.

On the other hand, pressure vessels may be subjected to life-degrading forms of corrosion, rust, mechanical damage, high and low extremes of temperature, and other unknown conditions. The pressure vessel is required to be inspected and tested for specific applications, but unless it is serviced by a licensed dealer, maintenance and testing of the vessel may in practice be ignored. The higher safety factor for pressure vessels compensates for the difference in operating conditions.

Failures of pressure vessels, aircraft, and other structures designed with safety factors have led to the restudy of the concept and its faults. One major realization was that material strengths and applied loads are not constant values. Theoretically, a safety factor—when this ratio is greater than one—is the strength of the structural components divided by the applied load. However, the actual strength of a structural member, such as a steel rod, will generally vary from the mean or nominal strength. The applied load or stress also may vary. When the stress exceeds the strength, a failure will occur. The variations of load and strength and the mathematical expression for probability of failure when the load exceeds strength are shown in Fig. 9-9. From the example of Fig. 9-9
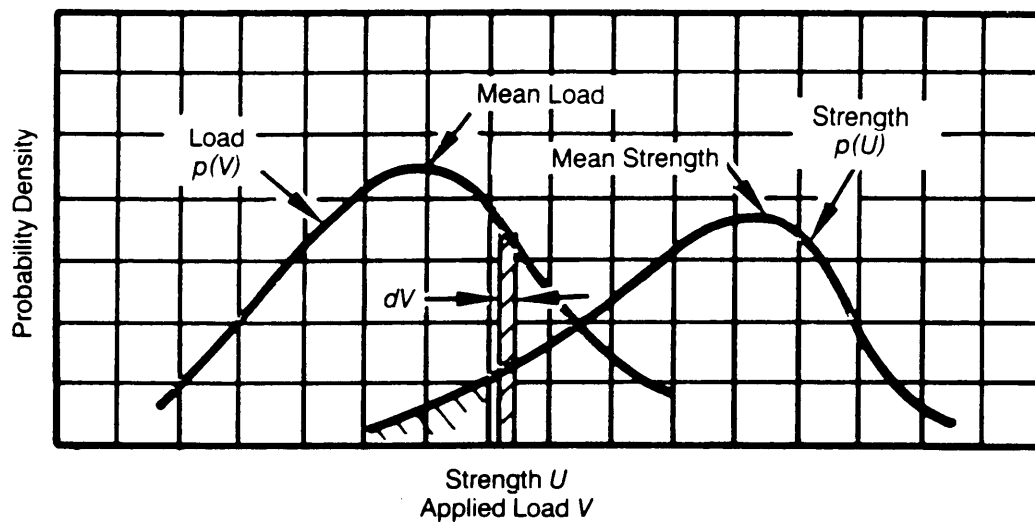
$$P_{\nu} = p(V)dV \qquad (9\text{-}10)$$

Figure 9-9.   Probability of Failure Due to Load and Strength Variations (Ref. 17)

$$P_U = \int_{U=0}^{U=V} p(U)dU \qquad (9\text{-}11)$$

where

   $p(V)$ = probability density function of applied load V

   $p(U)$ = probability density function of material strength U

   P_V = probability of applied load lying between applied load V and $(V + dV)$

   P_U = probability of material strength levels lower than material strength U

   V = applied load

   U = material strength.

The incremental probability of failure dP_c from the probabilities of Eqs. 9-10 and 9-11 is

$$dP_c = p(V)dV \cdot \int_{U=0}^{U=V} p(U)dU. \qquad (9\text{-}12)$$

The total probability of failure P is

$$P = \int_{V=0}^{V=\infty} p(V) \cdot \int_{U=0}^{U=V} p(U)dUdV. \qquad (9\text{-}13)$$

Numerous factors can create the situation in which load exceeds strength—e.g., inadequate designs, production deficiencies, environmental effects, or overloads due to errors regarding mission requirements. An example of inadequate design might occur if the designer did not call for the elimination of a sharp inside corner in a component. In such case, the concentration of stress at the

corners, when the item is under load, becomes far greater than the stress considered in design. If a part is gouged or scratched during manufacture or maintenance, that error may not only produce a sharp corner or a narrow area with a concentration of stress, but it may also remove metal and lessen the strength of the part.

Designers can reduce the probabilities of failures by increasing the nominal strength of the structure (moving the $p(U)$ curve in Fig. 9-9 to the right), reducing the nominal load (moving the $p(V)$ curve to the left), or both. In addition, designers may be able to incorporate design features that will decrease the loads and stresses that will apply, e.g., by minimizing vibration. Manufacturing personnel can increase the strength by use of improved production processes and stricter quality control.

The tails of the load and strength distribution curves shown in Fig. 9-9 reach to infinity. Their point of intersection can never be eliminated statistically, but it can be eliminated practically. This will occur when the maximum load, or stress, will not exceed the minimum strength. When minimum strength exceeds the maximum load, or stress, a safety margin is said to exist. The safety margin may be expressed in one of two ways: (1) as a ratio of minimum strength to maximum load or (2) as a condition that the applied stress will not exceed 90% of the yield strength. The analyst can review the criteria to determine the safety margin used for the design and later—if tests are conducted—to determine whether results indicate that the criteria have been met.

9-2.7.2   Electrical Components

Designers of electronic systems also tend to use longer lasting components than are normally required, but they generally call the process "derating" rather than the use of safety factors. Derating can be done in a number of ways—e.g., using components with capacities or capabilities greater than those required under the existing operating conditions, improving the operating conditions to

increase the capacity and reliability of the components, or reducing the load on the components.

9-2.8 WARNING DEVICES

Warnings, as a method of minimizing accident-causing failures, are used to apprise personnel of hazards, equipment problems, and other noteworthy conditions so that they can make correct decisions and avoid accidents.

9-2.8.1 Introduction

The law requires that the users of a product be provided with warnings to inform them about any dangers the product may pose that are not obvious. Failure to warn is, in itself, considered a defect by the courts. Therefore, a product can be considered defective by design, manufacture, failure to warn, or any combination of the three.

Some types of warning devices provide a continuous message; others are activated only when a hazard arises. Some warnings may be provided by manufactured devices; others are provided by an abnormal operating characteristic—e.g., temperature and/or vibration—of the equipment. Much information can be passed through the medium of warnings, e.g., signal lights can indicate either a hazardous condition or the safe, or "go", condition.

9-2.8.2 Label Versus All Human Senses

Numerous methods are available for alerting and warning personnel of dangers. Warning labels—informing users that potential dangers exist in a system—require use of the visual sense and interpretation of the warning message. However, the extensive use of labels and the specialized discipline for proper design of the labels place them in a separate category. Warning labels are discussed in par. 9-2.9.

Other methods of providing warnings may be categorized by the human senses that receive the warnings as follows: visual, auditory, olfactory, tactile, and gustatory. Many of these warnings are far more effective than labels and thus are used in more critical situations. The examples cited in the paragraphs that follow point out ways by which warning devices have been developed to trigger each human sense. These examples, however, constitute only a few of the many current applications.

9-2.8.3 Visual Warnings

Vision is the principal sense whereby information on the existence of hazards and dangers is transmitted to personnel. Among the numerous visual warning methods and devices are

1. *Illumination*. The location of an existing hazard is lighted more brightly than surrounding, less hazardous areas to focus attention upon that location. The illumination of obstacles may reduce the possibility of persons or vehicles running into the obstacles. Sometimes spotlighting the equipment will also provide an additional benefit, namely, security. Well-lighted weapon storage discourages unauthorized entry and facilitates the task of security personnel in observing the presence of danger.

2. *Discrimination*. A structure, a piece of equipment that moves, or a fixed object that could be struck by a moving vehicle may be painted either a bright, distinctive color or in alternating light and dark colors. Common examples are painting emergency vehicles so that they can be readily seen, painting alternate color bands on propellers, painting curbs not otherwise readily visible, and painting alternate color bands on vertical posts installed to protect other devices such as water hydrants, meters, or pedestrian rights-of-way. Recently the traditional red for fire trucks has given way to yellow and international orange so that the vehicles can be seen and recognized more readily. Operating areas for metalworking equipment where hazards exist are painted so that they can be distinguished from the protected areas. Piping and cylinders for toxic, flammable, or corrosive gases or liquids are color coded to indicate the hazards involved. Various grades of aviation gasoline are dyed different colors for identification by color coding, e.g., gasoline containing tetraethyl lead contains a red dye. Accumulations of the red dye at connections and joints in a fuel system also help to show where there are leaks since the dye remains after the gasoline evaporates.

3. *Signal Lights*. Colored lights are a common method of identifying the existence of hazards. These lights may be fixed or moving, steady or flashing. In general, the colors and their intended meanings are

   a. *Red*. Existing danger, emergency, malfunction, error, stop

   b. *Yellow*. Impending danger, marginal condition, caution, proceed slowly

   c. *Green*. Satisfactory conditions, proceed, ready, function activated properly, parameter within limits

   d. *White* (when used on an indicator panel). System available, operation in progress.

Flashing or moving lights are used to attract attention and to indicate urgency. When oscillating locomotive headlights were developed, they became much more effective as warning devices than fixed lights were. For this same reason, swinging or flashing red lights at railroad crossings are also more effective than fixed lights. Flashing lights are also used on fire trucks, emergency vehicles, and aircraft. Aural devices improve the effectiveness of flashing lights. (See par. 9-2.8.4.) Nonflashing fixed lights also attract attention but to a lesser degree. Highway accident statistics indicate that the likelihood of the occurrence of an accident is reduced when drivers keep their headlights on during daylight. Another effective nonflashing light signal is the reflector used on barriers, road shoulders, and as lane markers. The reflector is especially effective on the pedals and spokes of a bicycle wheel because they appear to be a moving light when illuminated by vehicle headlights.

4. *Flags and Streamers*. These have frequently been used as alerting devices to show that protective covers are installed on Army aircraft and helicopters. Streamers are also used to call attention to the fact that safety pins or plugs—which must be removed prior to use—are installed in various types of ammunition. Tiny "flags" appear in air vehicle instruments to indicate that the instruments are no

longer to be relied on due to a malfunction. On one type of smoke detector, a metal flag pops out to warn that the battery has been removed or is discharged and that the device is inoperative. Flags on ships may indicate hazards such as the loading or unloading of explosives or sickness aboard. A red flag or streamer marks the end of a long load protruding from the back of a vehicle. Flags are also attached to wires, ropes, or cables to attract the attention of personnel or vehicles that might otherwise run into them. Tags are attached to components to indicate that they require repair, that they should not be used unless special precautions are taken, or that they have malfunctioned. A tag should *not* be used, however, to indicate that the system has been inactivated and should not be operated. Flags of different colors and designs are used to mark the hazardous areas in a military situation such as active target and range areas, minefields, and uncleared ammunition impact areas. Other types or colors of flags will mark the safe areas or paths.

5. *Labels.* These are discussed in detail in par. 9-2.9. They may be attached to or painted on equipment that contains a hazard. They may point out high voltage, phase, and power requirements in electrical equipment; give load, speed, or temperature limitations; warn against pressure hazards, state the need to wear protective equipment when servicing pressurized equipment; point out the means of disposal if the equipment is radioactive; or indicate low headroom. Lift points may be painted on structural elements, and "No Step" may be marked on fragile parts of equipment such as the flaps on light Army aircraft. Color-coded pipelines and cylinders previously mentioned could also be labeled to indicate the contents of the lines.

6. *Signs.* The most common signs are fixed signs, such as road signs to point out curves, intersections, narrow bridges, slippery roads, and other hazards. Signs indicating a specific hazard are consistently and distinctively shaped and colored. Many countries now use international symbols that can be understood by persons unfamiliar with the language. Included in this category are signs identifying tanks or other containers of hazardous materials—e.g., flammables, explosives, toxic gases, and corrosives. Pictorials add to the effectiveness of the message the sign portrays. Consoles for electrical equipment sometimes have electrically activated signs to indicate when a critical malfunction or hazard exists or when a specific action should be taken. Some vehicles have backlighted signs that illuminate to warn drivers when there has been a brake failure or the brake has not been released, less than one quarter of a tank of fuel remains, or a seat belt is not fastened. Some equipment have backlighted signs to indicate that a malfunction has occurred and to direct the operator to that component.

7. *Procedural Notes.* These notes include warnings and cautions inserted in operation and maintenance procedures, instructions, manuals, and checklists. The notes alert personnel to hazards; to the possibilities and effects of errors; to special care or actions that must be taken; and to protective devices, clothing, or tools that must be used. Any procedural step in which an error or

malfunction could result in injury or damage should be preceded by a precautionary note. The warning or caution in the instruction manual, handbook, or list should correspond to the warning or caution label on the equipment; conversely, any hazard that calls for a label should be mentioned in the instructions.

9-2.8.4 Auditory Warnings

In some situations visual warnings alone are inadequate. Sometimes personnel are so occupied that they fail to note visual signals even though the signals are within view. Persons may also move about, often into positions where they cannot see a visual warning. A bright visual sign can be seen over a greater distance than an auditory signal can be heard, but an auditory signal could be more effective within its range. A siren is an excellent example.

Auditory signals can be coded to indicate the type of emergency that exists and the emergency procedure to be followed. Auditory signals can also be used to call attention to a visual display that will provide detailed information on the condition constituting a problem.

MIL-STD-1472 (Ref. 3) offers guidance on auditory displays and warnings. It recommends that auditory signals be used when

1. The information to be disseminated is short, simple, transitory, and requires immediate response.
2. The usual mode of warning by a visual display is restricted by other visual demands on the operator, variable or limited light, operator movement, other environmental considerations, or anticipated operator inattention.
3. The criticality to respond makes a supplementary or redundant alerting signal desirable.
4. It is desirable to warn, alert, or cue the operator to subsequent additional information or response.
5. Custom or usage has created anticipation of auditory signals.
6. Voice communication is necessary or desirable.

Commonly used auditory warnings are sirens, buzzers, bells, or alarms on timing devices that indicate when a specific period of time has passed or that the time has arrived to take the next step in a sequence. Some compressed-air respiratory packs contain alarms that sound when the pressure level in the pack decreases to a predetermined level or after a preset time has passed. Sometimes recorded vocal messages are also played over a loudspeaker system, or an individual warns another by a direct shout.

9-2.8.5 Olfactive Warnings

Odors can be detected only when certain gas molecules affect the small, sensitive area—approximately 645 mm^2 (1 in.^{2})—of the nasal cavity. Some gases have no odor; others are so strong that even small amounts may sicken the person affected. The body has the ability to desensitize itself to odors fairly rapidly. This ability, in one sense, is an advantage—odors generally constitute little problem after a person has become desensitized to their presence. In addition, the ability to detect odors varies considerably

with individuals and their habits (smoking degrades the capability). These factors reduce the advantages of odorants for warning purposes except for short exposure periods and when desensitization has not already occurred. Nevertheless, odorants are used successfully as a warning medium as indicated by the following:

1. Some poison gases, such as mustard gas— used extensively in WWI—have very distinct odors, both to give warning and to identify the type of gas. Some of the newer materials, such as nerve agents, have little or no detectable odor.

2. An odorant may be added to highly flammable and explosive gases having no odor of their own. Natural gas, from which sulfur compounds have been removed, has no odor. To reduce the possibilities of fires and explosions from leakage of natural gas in homes or shops, a small amount of a gas with a strong odorant—usually a mercaptan—is added. The added odorant is so powerful that any leak would be readily detectable even though the concentration of flammable gas is still far less than that required to start a fire or explode.

3. Overheated equipment usually produces a telltale odor. A lubricating oil with a fairly low vaporization temperature can serve as an olfactive warning if overheating from excessive friction volatilizes it and makes it readily detectable. This method was once used in journal boxes on railroad car wheels. A material was added that vaporized if a bearing overheated; the vapor pinpointed the problem for any crewman making an inspection during a stop.

4. The presence of fires can be detected by the odors of gas produced from combustion. Materials, such as plastics and rubber, have characteristic odors that indicate what substance is burning and its possible location.

9-2.8.6 Tactile Warnings

Vibration is the chief tactile means of providing warnings. Excessive equipment vibration warns that an operation is not normal and is degrading toward a failure. Examples are a rotating shaft or bearing that is beginning to wear or the rough running of an engine. The roughness may be caused by a worn part, incorrect ignition timing, low-grade fuel, or a lubrication failure. The magnitude of the vibrations usually indicates the severity of the problem.

Vibration-inducing devices provide warnings on streets and highways. For example, raised lane markers cause a vehicle passing over them to vibrate and the tires to respond with an uncharacteristic noise. These markers may indicate that the vehicle is too close to a shoulder or to a center divider, that the vehicle is crossing into another lane, or that the vehicle is approaching a stop sign or signal. A driver who dozes off may be awakened and alerted to the danger.

Control columns and pedals on aircraft with electric or hydraulic flight control subsystems are generally equipped with "feel" devices such as control shakers that apprise the pilot of impending hazardous aerodynamic conditions.

Temperature sensing is another method of providing

warning through tactile sensation. Maintenance personnel may be able to determine whether or not a piece of equipment is operating improperly by feeling it with the hand. An increase in temperature may warn that the equipment is malfunctioning and requires maintenance, that it lacks the capacity for normal requirements, or that it is handling abnormal loads. This method is particularly useful for checking equipment housed in an air-conditioned facility.

9-2.8.7 Gustatory Warnings

The sense of taste is probably the least important to the military as a warning mechanism. Taste has been used to determine whether a food, drink, or other material taken into the mouth is dangerous or contains a dangerous contaminant. Medicines that might be dangerous to children may have an additive to give the medicine a bitter taste to discourage a child who sampled the medicine from taking more than one swallow. If a food or drug can deteriorate, the accompanying instructions will recommend that it be discarded if it tastes bitter, salty, acidic, or unusual.

9-2.9 LABELING

Labeling is a very special type of visual warning and instruction mechanism. The proper design of labels must consider many factors. Most important is the category of people—operators, maintenance personnel, or passersby— whom the labels are to warn or instruct. Personnel outside the expected category must also be considered since there is normally no guarantee that only the expected people will confront the labeled equipment. Differences in language, education, experience, skills, and even motivations must be a part of the total label design considerations.

9-2.9.1 General

Labels are a type of visual warning device, a means of alerting personnel to the existence of a hazard, and they are probably the most common means now in use of alerting personnel to equipment hazards. In spite of this—and of the fact that they have been used for many years—labels are often inadequate as a tool to prevent accidents or to satisfy the legal duty to warn of hazards. Traditionally, the label has been designed and placed in a specific location on a piece of equipment at the direction of the design engineer. The label has wording, colors, and style, which the designer thought would satisfy the requirement to warn. Unfortunately, unless the designer had the assistance of a qualified safety engineer, the label probably lacked one or more of the necessary elements described in par. 9-2.9.2 and thus constituted a design deficiency.

9-2.9.2 Design Requirements for Labels

All manufacturers have a legal duty to warn of any obscure hazards accompanying the use of their products. (Employers have a similar duty to warn employees of

hazards in the workplace.) A failure to warn of a hazard that results in an injury has long been considered a negligent act. In the last 20 yr, a failure to warn "adequately" has been considered a design defect. The word "adequately" is open to interpretation and cannot be resolved except by a jury or court in each individual case where "failure to warn" is the issue. There are, however, certain basic items of information that a warning label must contain in order to be considered adequate in any case, i.e.,

1. A key word that will attract the attention of the user, maintenance man, or other person who might potentially be in danger of the specific peril and risk involved

2. A description of the hazard against which to be guarded

3. A description of the action to be taken to avoid injury or damage

4. A brief statement of the resultant consequences if the indicated action is not taken

5. In some instances, it is also necessary or advisable to indicate the remedy or corrective action to take if an injury occurs due to ignoring the warning—e.g., antidote for poisons and instructions to administer cardiopulmonary resuscitation (CPR) in the event of an electric shock.

At the present time DoD documents cite requirements for observance of standards, codes, and specifications that do not include or explain all of the elements required in legally sufficient warning labels. For example, MIL-STD-454 (Ref. 2), Requirement 1, par. 9.2, stipulates that ANSI Standard Z35.1 (Ref. 18) be used even though the standard was prepared for industrial facilities and is not entirely satisfactory for military requirements. In addition, warning signs or labels for voltage potentials between 70 and 500 V are to read "CAUTION—(insert maximum voltage applicable) Volts". For potentials over 500 V, the word "DANGER" is used instead of "CAUTION", and the words "High Voltage" are added. The alerting word "WARNING" is not found in either Requirement 1, MIL-STD-454 (Ref. 2), or ANSI Z35.1 (Ref. 18).

In Requirement 27, par. 5.1, MIL-STD-454 (Ref. 2), the labels for batteries are to use the alerting word "WARNING". ANSI Standard C95.2 (Ref. 19), which is also cited in Requirement 1 of MIL-STD-454 (Ref. 2), states that to indicate the presence of biologically hazardous levels of electromagnetic radiation, the word "WARNING" will be used. MIL-M-38784 (Ref. 20) stipulates that warnings to be included in operating or maintenance procedures will use the words "CAUTION" or "WARNING". The word "DANGER" is not included as an alerting word.

It would be helpful to design groups if a concensus could be established for the various warnings and if the standards, codes, and specifications were coordinated accordingly.

9-2.9.3 Recommended Labeling Procedure

Since Government specifications or standards are not too specific on the use of one standardized type of warn-

ing for nonobvious hazards, designers and analysts need guidance to produce acceptable warning labels. In the implementation of any guidelines, it is of paramount importance to analyze the hazards carefully to insure that the selection of the intensity level is appropriate for the possible consequences. For example, "WARNING" should not be the alerting word when the possible consequence is severe injury or death. Conversely, "DANGER" should not be used when the possible consequence is a minor injury. The obvious misuse of the alerting word to announce potential hazards will breed contempt for all signs. It is, therefore, recommended that designers use, and analysts verify the use of, the following guidelines:

1. *Alerting Word.* When not otherwise specified by a Government requirement, e.g., Refs. 2 or 3, the alerting word will be

a. CAUTION. For a notice requiring correct operation or maintenance procedures or practices to prevent minor damage to or destruction of equipment or creating a minor personnel hazard. An example is a label advising that a cooling system be turned on before the operating equipment is turned on to avoid overheating and damage.

b. WARNING. For a notice requiring correct operation or maintenance procedures or practices to prevent personnel injury or loss of life because of a potential, but not imminent, hazard. An example is a label on an access panel to electrical equipment that might shock a person.

c. DANGER. For a notice indicating immediate danger or peril capable of producing injury or loss of life. An example is a label near electrical equipment where a person might receive a shock.

2. *Color Coding.* The proper use of color coding is of major importance in an effective label system. Colors to be used for labels should be those stipulated in ANSI Z35.1 (Ref. 18) or other specified document. It is recommended that red be associated with DANGER, orange with WARNING, and yellow with CAUTION.

3. *Other Information.* Other legally required information pointed out in par. 9-2.9.1 should also be included: the key alerting word, the nature of the hazard, the action to be taken, the consequences of failure to heed the warning, and the corrective action for the injury warned against when the warning was ignored. Fig. 9-10 (Ref. 20) indicates the type of information that should be included for warnings in technical manuals. Information similar to that in Fig. 9-10, but perhaps somewhat more brief, should be provided on labels. Consideration should be given to portraying the hazard message pictorially. This aids non-English-speaking personnel to be alerted to the hazard.

4. *Location.* Warning labels should be located where they are obvious to and easily readable by the persons who are to be warned and as near as possible to the location of the hazard or on the barrier. Obscuration of the label by the accumulation of dirt or grease and the erasure of the label by mechanical action should also be considered in placement.

5. *Equipment and Manuals.* Labels on equipment must be consistent with the warnings in operation and

Figure 9-10. Examples of Warnings for Manuals (Ref. 20)

maintenance manuals. MIL-M-38784 (Ref. 20) requires the inclusion of a page in the front of the manual that presents the more vital warnings extracted from the remainder of the manual. A safety summary that includes all general precautions and all warnings and cautions (Ref. 20) will also be provided somewhere in the manual.

6. *Logos and Symbols.* Logos and symbols (or decals) are often highly effective for alerting personnel to hazards and of reminding them of the equipment to be used and what actions are to be taken or avoided. Many of these logos and symbols were developed by professional panels composed of representatives from various professional societies. They may not have been developed

for military applications; however, many of them, such as the "DANGER—FLAMMABLE LIQUID" decal, apply equally well to military materiel, and others are readily adapted. (See par. 9-2.9.)

7. *Understandability.* Labels should be simple, easy to understand, not open to misinterpretation, and composed of as few words as possible. Their wording, for easy reading, should be directed toward the educational level of the persons to be warned. If they are to be read by persons from different countries, the labels should be multilingual.

8. *Consistency.* Different words, signs, or symbols to convey the same idea should be avoided because they lead to confusion.

9-2.9.4 Sources of Logos and Symbols

Commonly used logos and symbols should be relied upon wherever possible. Generally, the emphasis has been upon providing information in a form other than words. Many logos and symbols have been developed and used internationally for purposes other than labeling military equipment; however, this technique can be adapted for use with military equipment. For example, traffic signs frequently have a slanted line crossing out the figure or symbol to indicate something that is prohibited or should *not* be done. Department of Transportation labels for hazardous materials, by means of symbols that could also be used on equipment labels, indicate whether the contents of a container are flammable or corrosive. The Bureau of Radiological Health has developed and prescribed both the widely used radiological hazard symbol and laser symbol (Ref. 21). Some military standards contain requirements for the color coding and marking of materials, containers, and other equipment (Refs. 22 and 23).

In situations where commonly used logos or symbols do not exist, some companies have developed their own. Fig. 9-11 (Ref. 24) was developed by an Army contractor. Contractors and certain engineering societies (Refs. 24 and 25) have developed other logos and symbols for use by their members. The National Bureau of Standards has done original work in developing warning logos and symbols (Ref. 26). If suitable known logos or symbols do not exist, designers and human factors engineers can develop their own by using Refs. 24 and 27 for guidance.

9-2.9.5 Labels: A Last Resort

"When all else fails, read the instructions" is a tongue-in-cheek comment that also applies to warning labels. Instructions and labels are often ignored until trouble is encountered. For this reason, only as a last resort should persons be relied upon to read labels as a safety measure. The presence of a warning label on a piece of equipment indicates unquestionably that the designer knows that a hazard exists. That knowledge imposes a requirement that the hazard be eliminated or controlled if possible so that the warning will not be necessary. If, after such efforts, the need to warn still exists, the label is not only

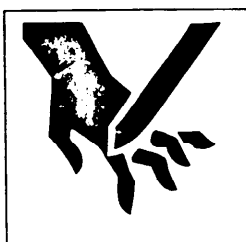(A) Ear Protection
Required
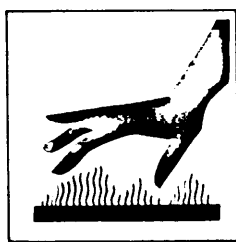
(B) Hot Surface
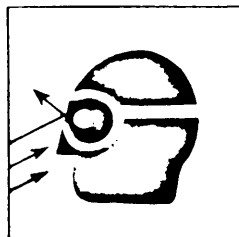
(C) Projectiles–Eye
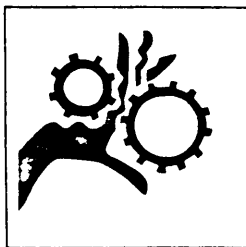Protection Required

(D) Falling Objects

(E) Electrical Shock

(F) Keep Hands Out–
Sharp Objects

(G) Slippery

(H) Keep Hands Out–
Gears

Figure 9-11.   Warning Symbols (Ref. 24)

Reprinted with permission. Copyright by FMC Corporation, 1980.

justified but required. No designer, however, should use the warning on a label as a substitute for good design.

9-2.10   MINIMIZATION AND CONTAINMENT OF INJURY AND DAMAGE

As long as a hazard exists, there is always the possibility, however remote, that an accident will occur, but there is no way of knowing precisely when it will occur. Therefore, designers must fully explore ways to minimize potential injuries and damage. Cost considerations and functional requirements may make it impractical to provide complete protection, but many safeguards can probably be incorporated. Some of the protective methods are physical isolation, personal protective equipment, and energy-absorbing mechanisms (discussed in pars. 9-2.10.1 through 9-2.10.3), escape and rescue (discussed in par. 9-2.11), and weak links (discussed in par. 9-2.12).

9-2.10.1   Physical Isolation

Isolation has already been discussed (par. 9-2.3) as a means of preventing accidents. It is also frequently used as a method of minimizing damage from a violent release of energy as a result of an accident. Isolation techniques rely upon distance, deflection, and containment. These techniques limit injury and damage by preventing the consequences of an initial, unwanted event from adversely affecting adjacent personnel and/or materiel. A brief discussion follows:

1. *Distance.* A common method of physical isolation involving explosives is to locate the site of a possible accident far from personnel, material, and structures. Explosive safety quantity-distance criteria are applied, and the amounts and types of explosive that can be located or stored at specific distances from other critical items, inhabited areas, public roads, or structures are determined. The purpose of the criteria is to isolate the explosives so that an accidental detonation in one location will not result in sympathetic detonations in adjacent storage areas.

2. *Deflectors.* Isolation may also be provided by deflectors. Barricades between explosives and inhabited or other critical buildings are doubly effective because they absorb part of the energy of an explosion and deflect the remainder upward where it will do no harm. Roofs are built less strong than sidewalls to permit the force of the explosion to be directed vertically rather than laterally.

3. *Containment.* Containment techniques are other common means of isolation for damage control, e.g.,

a. Additional hazards generated by a mishap can be contained. For example, to limit the spread of a magnesium fire resulting from an accident, water should be sprayed on adjacent areas to cool them and thereby prevent ignition of other materials and minimize damage from the intense heat. Ditches, or moats, can be dug around storage tanks of liquid toxic agents or flammable substances to contain a leak or spill.

b. An operation may become uncontrolled as the

result of an accident, but damage and injury can be avoided by limiting the effects. A tire may blow on a vehicle on a test track and cause the car to spin out of control in the vicinity of test personnel. Suitable barriers should be in place to confine the vehicle to the limits of the test area so that no other personnel are injured nor other equipment damaged.

c. Personnel can be provided protection. Techniques involving energy-absorbing mechanisms for this purpose are discussed in par. 9-2.10.3. In some systems, certain areas or structures can be designated as "safety zones" where personnel will be safe from the hazards generated by an accident. The consequences of the original mishap are confined to the area of the primary structure or of the equipment involved in the mishap. Therefore, personnel not trapped in the actual impact or damage area are protected by containment.

d. Materials can be protected by methods similar to those for personnel. In addition, containers of metal, plastic, or other impermeable or impenetrable substances are effective in minimizing damage to the materials stored within if a mishap occurs. For example, waterproof containers will protect the contents from damage as the result of an accidental leak or a flood. The water, in effect, is being contained on the outside of the stored material.

e. Critical equipment can be similarly protected. For example, a pump whose operation may be required in an emergency, such as a flood, can be hermetically sealed so that it will run underwater. The water is contained outside the pump housing.

9-2.10.2 Personal Protective Equipment

The use of personal protective equipment is another way to minimize injury resulting from accidents. The user is provided with a limited, controlled environment that isolates him from the adverse effects of a hazard. Personal protective equipment consists of those garments or devices that are worn for protection against an accident or an unfriendly environment. They may vary from a simple set of earplugs to an astronaut's space suit complete with life support equipment. The earplug user is isolated from noise and its adverse effects; the astronaut is isolated from space hazards.

Personal protective equipment may be required to safeguard personnel against harmful environments created by the operation being performed, such as welding, or resulting from mishaps. The equipment must be adequate to protect its user under the worst possible foreseeable conditions. Since conditions are specific, equipment that is suitable for one set of circumstances may not be suitable for another. For example, a gas mask that provides protection against chlorine or other toxic gases would not provide protection against the absence of oxygen. For the latter case, an air pack or oxygen generator is necessary.

The needs for personal protective equipment can be divided into the following three categories:

1. *For Scheduled Hazardous Operations.* Operations may have to be conducted in environments that could be as damaging as if an accident had occurred because the hazard cannot be eliminated. The conduct of inspections and scheduled and/or preventive maintenance in a hazardous area is an example. Protective equipment is provided for numerous hazardous operations and is to be worn while the operation is being conducted. The use of personal protective equipment, however, must not be substituted for good design, hazard elimination or control, and safe operating procedures. For example, a person working in a confined space containing a poisonous atmosphere should not be required to wear respiratory protective equipment if the space could be ventilated and monitored to insure a normal, breathable atmosphere.

2. *For Investigations and Corrections.* Detection equipment may indicate, or personnel may suspect, that an environment is dangerous. It may then be necessary for someone to enter the area, determine the source of the contamination or other dangerous condition, and take corrective action. In some instances, the nature of the hazardous material may be known, such as during the neutralization or decontamination of a leak or spill of a toxic, corrosive, or flammable liquid. At other times, the exact nature of the contaminants or their concentrations may be unknown or uncertain. Personal protective equipment for this purpose must be capable of providing protection against a broad spectrum of potential hazards.

3. *For Emergencies.* An emergency generates the severest requirements for protective equipment. When a contingency has become imminent or has occurred, the next few minutes may make the difference between control or catastrophe. Accordingly, the amount of reaction time to suppress or control the hazard, and to minimize damage and injury, is extremely important. To be effective, emergency protective equipment

a. Must be simple and quick to use, particularly under the stress of the emergency

b. Must be highly reliable and effective against a broad variety of hazards

c. Must not unduly degrade the agility and visibility of the user

d. Must not constitute a hazard itself.

Bearing all this in mind, remember that emergency equipment should only be considered as backup, i.e., as a redundant arrangement to be used only if more preferable methods of accident prevention or damage and injury control are not possible.

Product designers must insure that equipment designed or selected for personnel protection is suitable for the hazardous conditions that might be encountered. The equipment must function as intended or the user could be exposed to a second mishap with a much higher probability of fatality. In specifying such equipment, the analyses of the designs, the hazards involved, the procedures for use, and the safeguards to prevent impairment of performance must be even more stringent than for equipment used for normal mission purposes. The designs must be extraordinarily easy to apply or operate because the possibilities of human error are increased due to the stress that personnel are subjected to during emergencies.

The design and testing of protective equipment should insure to the greatest degree practical that

1. It will not deteriorate rapidly in storage or in the hazardous environment where it is supposed to provide protection.

2. It will not become brittle or crack because of the flexing action in normal movement, temperature extremes, sunlight or other radiation, or other deleterious environments.

3. It is easy to clean and decontaminate.

4. Clothing designed to protect against toxic or corrosive gases or liquids is impermeable.

5. Coverings that might be exposed to fire are noncombustible or self-extinguishing.

6. Facilities for the storage of emergency protective equipment are located as close as practical to the area where the equipment is likely to be needed. However, the storage facility must not be so close that the condition generating the emergency will affect the equipment or prevent personnel from reaching it. Storage areas should be easily accessible and marked for quick identification, and their locations should be clearly marked in published operating procedures.

7. Brief, clear instructions should describe proper methods of fitting, testing, and maintaining personal protective equipment.

9-2.10.3 Energy-Absorbing Mechanisms

Energy-absorbing mechanisms can protect personnel, materials, and sensitive equipment from the effects of impact. For example, seat belts, bumpers, and padded interiors reduce injuries to occupants of vehicles involved in accidents. Plastic foams, rubberized horsehair, and similar cushioning materials in storage or transport containers protect items that would otherwise be damaged if the container were dropped or jarred. Cushioning materials and the design of protective cushioning configurations are thoroughly discussed in Chapter 7, Ref. 28.

To protect personnel, one of the principal protective features involved is "crashworthiness", which is predicated on the principle of energy absorption. (See par. 9-2.11.) In addition, shoulder straps, seat belts, and other harnesses restrain and isolate occupants and equipment in a vehicle so that they will not be thrown about and injured or damaged in an accident.

9-2.11 ESCAPE AND RESCUE

A contingency may continue to deteriorate until a point is reached at which the personnel must abandon the area and sacrifice the equipment or structures to avoid injury. This is the point of no return. Following unsuccessful efforts to recover from the emergency, to suppress the hazard and any damage that could result, to isolate adverse effects, and to restore normal conditions, it may be necessary to abandon ship, bail out, eject, or in some other way leave the danger area. For such situations, escape, survival, and rescue procedures and equipment are literally vital because lives depend on them. "Escape" and "survival" refer to efforts by personnel to save themselves by using their own resources; "rescue" refers to efforts by other personnel to save those endangered by the emergency.

The importance of escape, survival, and rescue equipment is paramount for those situations in which they are necessary. However, such equipment should be considered and used only in cases of last resort. To avoid last resort situations, design engineers must do their utmost to eliminate or minimize those conditions that could result in accidents. System design should maximize the use of safety devices and procedures to avoid or eliminate the necessity of using escape and rescue equipment. In numerous cases, however, hazards cannot be eliminated entirely because unforeseen accidents will occur and, consequently, escape and rescue equipment must be provided.

In some cases, escape may be a fairly easy process; under only slightly different conditions, escape may be impossible. For example, when a large American-made helicopter crashes, it has a tendency to flip onto its right side due to the reaction of the rotors' striking the ground. (Some foreign-made helicopters have rotors that turn in the opposite direction, and these helicopters tend to flip over on the left side.) If the right side had the only exit door, escape generally would be impossible. In a related problem, forward impact caused the helicopter door to slide shut and jam, which trapped the passengers. That problem was corrected by using a more secure latching device.

The same concern relative to exit doors applies in all vehicles, both ground and air. An automobile collision may cause the car doors to jam such that the occupants have to be rescued. If the occupants are badly injured or if there is a fire, survival depends on the speed with which they can be removed from the damaged vehicle. To afford rapid egress, aircraft are generally provided with multiple exits to permit evacuation of personnel within a specified time even when a number of the normal escape routes are blocked.

The designs and devices to permit escape after a collision are an aspect of crashworthiness, an important consideration in the design process. Crashworthiness is a three-part concept:

1. Protection by isolating the person, generally against impact and other energy effects and against the hazard of fire

2. Escape, i.e., permitting the person to leave the vehicle and to reach safety from any hazards resulting from the crash (See par. 9-2.11.1.)

3. Rescue operations, i.e., when the person cannot escape by his or her own efforts. (See par. 9-2.11.2.)
Designs for the escape and rescue aspects of crashworthiness, therefore, include such items as escape doors and panels, nonjamming doors, knockout windows, and breakaway sections. This last method involves designing a vehicle so that on impact it will break apart at specific locations to provide large openings for the escape or rescue of the occupants.

It is evident that escape and rescue devices must be treated as critical items of the system. They must be analyzed and tested extensively to insure that they will meet their intended purposes with very low probabilities of failure. Such equipment is subject to hazards, as was the basic operative system, but there is one major difference: When escape and rescue devices become necessary,

the control of a hazard has already been lost, and this makes the initial danger level much higher.

The failure of escape, survival, or rescue equipment may be worse than if that equipment had not been supplied. In some instances, the items themselves have injured the users because of their poor design or manufacture. In a crisis, failure or inadequacy of the escape, survival, or rescue equipment produces traumatic shock over and above that produced by the original mishap. In addition, the time lost in establishing that the equipment does not work or works improperly, then determining an alternative course of action, and finally taking that action under stress combine to reduce the chances of success. To make matters worse, alternative courses of action may now be impossible because the time to implement them has been lost.

The need for escape and rescue equipment and procedures must be established by contingency analysis. Once this task is done, the equipment must be selected carefully. The equipment must be analyzed to insure that it will fulfill all foreseeable needs and that procedures for its use are readily available and adequate. The equipment should be studied in detail through failure mode and effects analysis (FMEA) or other methods. A test program must be developed to insure that the items will function under expected conditions, that they will satisfy established requirements, and that procedures are adequate. Tests also should be conducted under worst-case conditions to determine whether or not the equipment can be operated and the procedures followed by a partially incapacitated person.

Sometimes escape and rescue equipment that is initially suitable for emergencies is not properly maintained. Consequently, it deteriorates and no longer functions as it should. Therefore, procedures must be established for both proper use and maintenance, and replacements must be made whenever needed.

9-2.11.1 Escape and Survival Procedures and Equipment

An example of the distinction between equipment for escape and equipment for survival is a jet pilot's emergency equipment. The ejection seat helps the pilot to escape from the aircraft; other devices enable the pilot to survive in the new environment. To survive the high-velocity air blast at ejection, the pilot must be protected by a shield or capsule. A parachute is then required so that the pilot can survive the fall to the ground. A temporary supply of oxygen and insulation against the cold may also be required. If the flight is over an ocean or lake, an inflatable life raft stocked with food and water would permit survival for an extended period. Other special provisions are required for flights over arctic, tropic, or jungle areas.

In Army tactical situations, large areas of the ground and its foliage may be contaminated with enemy chemical agents or even fallout from tactical nuclear weapons. To protect personnel from the effects of these chemicals or nuclear fallout, safety zones must be established and clearly marked. These safety zones are areas that have

been decontaminated or otherwise determined to be free of hazardous materials to permit personnel to move about in these safety zones without fear of exposure. Minefields, whether prepared by friendly or enemy troops, should also be treated as "contaminated" areas requiring safety zones and routes of passage. As the tactical situation moves forward, the clear routes through contaminated areas become supply routes and evacuation routes for whatever emergencies require rearward-moving traffic.

A contingency plan identifying the most likely safety zones and evacuation routes from danger areas should be disseminated to personnel in the immediate area. The plan should be based on an analysis to determine locations where personnel will be safe or where they can withdraw during an emergency. Protective structures or routes can be provided or designated beforehand to house personnel or enable their passage to safety under certain circumstances. Contingencies to be considered are

1. The likelihood that damaging effects can occur so rapidly that reaction or escape time will be minimal

2. The damage could be so extensive that there would be difficulty evacuating the area.

3. The number of affected personnel could be so great that some would be injured in the evacuation process. (In earthquake regions a common instruction is to take refuge under a sturdy table, desk, or similar piece of equipment if the building might collapse. Similar refuges can be used if a building is damaged by an explosion and in danger of collapse.)

Escape routes should be selected and then evaluated for capacity to handle the number of personnel who would use them. Routes and exits should be marked conspicuously so that they can be followed easily. (For peacetime situations, OSHA standards require the marking of routes, egresses, and exits.) The number of exits and egresses must be adequate for the amount of escape time and number of expected evacuees in an emergency, and that number of exits must take into account the possibility that one or more of them will be blocked. Consequently, alternatives must be established. Emergency lighting may be necessary if loss of the normal lighting system could throw the routes into darkness. Egress and exit signs must be lighted, with provisions for emergency power, in buildings with numerous corridors. Emergency lighting may also be required in buildings with no natural lighting.

9-2.11.2 Rescue Procedures and Equipment

In any emergency there is the possibility that the persons involved may not be able to escape under their own resources. Accordingly, provisions must be made for rescue by other personnel should the need arise. Rescues may be attempted by

1. Persons familiar with the equipment and its operation, hazards, and emergency devices

2. Personnel familiar with the hazards in general but not with the specific equipment. For example, a city fireman may be well-trained in fire fighting but may lack training in rescuing personnel from burning aircraft.

3. Untrained personnel who are unfamiliar with the equipment and hazards involved but who want to help.

Because the last two categories of personnel can, and do, provide vital assistance, it is essential to mark all emergency devices so that untrained volunteers can determine how and where to assist the persons to be rescued. Adequate design and suitable marking of rescue devices may mean the difference between a successful and an unsuccessful rescue attempt. An example is the set of latches on the outside of an aircraft to release the cockpit canopy. If these latches are conspicuously marked, all three categories of rescue personnel would be able to operate them. If the latches are not marked, only the personnel familiar with those particular latches may be able to operate them properly.

Rescue equipment must be foolproof—i.e., be so simple and reliable as to leave no opportunity for error, misuse, or failure—in an emergency, require little physical effort to operate, and be easy to understand when only a few words of instruction are provided. The instructions should be marked so that persons under stress can quickly find, identify, and understand them.

The time to study and develop suitable rescue devices and procedures is early in the acquisition process when contingency analyses should be made. The results of these analyses may determine whether or not the protective or rescue devices or procedures will require changes or additions. The need—discussed previously—for rigid analyses of escape and survival equipment because of their criticality is even more applicable to rescue devices. If an escape device fails, the user may become a casualty. If the rescue equipment fails, both the rescuers and the persons they are trying to help may become casualties.

Rescue equipment may be

1. Specifically designed for a system
2. General-purpose items that can be used for a wide variety of emergencies
3. Improvised from items built for other purposes.

An example of the first category is the emergency canopy release for an aircraft. An example of the second category is the crash truck on an airfield. An example of the third category is the use of helicopters for the rescue of people from burning aircraft. The helicopter was not made specifically for the purpose, but it was found that the downdraft from its rotor blades would blow flames away from the escape path of persons in the aircraft. That path can also be used by rescuers. A helicopter can also be used to extricate personnel from inaccessible locations.

Organizations using rescue devices and equipment should develop preaccident plans. Instructions must be written and training undertaken to insure that operators and rescue personnel understand and are proficient in carrying out rescue procedures. Scheduled practices using simulated emergencies also help to increase rescue proficiency. Investigations of many serious accidents have revealed that personnel died because of the lack of proficiency in the use of rescue equipment or because rescue personnel failed to follow established procedures.

9-2.12 WEAK LINKS

Of concern to designers and safety engineers are the components or materials that tend to fail more easily than others. This characteristic has been put to good use in many systems to limit damage when malfunctions, contingencies, or accidents occur. A "weak link" is incorporated into the system; it will fail before some other item fails and causes much more serious damage to equipment or injury to personnel.

The most common applications of weak links are electrical, thermal, mechanical, or structural types. Examples follow:

1. *Electrical.* Electrical fuses are incorporated into circuits to prevent fires or other damage caused by sustained overloads. The fuse contains a restrictive conductor made from a low-melting-point metal. If an overload occurs, possibly because of a short circuit, the heat generated by passage of the current overload through the fuse will cause it to melt and open the circuit. However, a fuse is no protection against an electrical shock.

2. *Thermal.* Boilers in portable steam cleaners may use thermal plugs as safety fuses that are normally cooled by the water in which they are submerged. If the water level should drop below the plug, it will no longer be cooled, and it will melt. This will provide an exhaust passage for the steam, and the pressure will drop. The level of the plug in the boiler is such that it will be uncovered well before an accident is imminent. Another application of a thermally activated device is in the sprinkler heads of a piped fire extinguisher system. The heat from any fire melts the metal that blocks the valve in the sprinkler head. The head opens and releases water (or gaseous extinguisher) to quench the fire.

3. *Mechanical.* Mechanical fuses may be pressure activated. The most common example is the safety diaphragm in pressure fire extinguishers. If the extinguisher overpressurizes because it is exposed to abnormal heat, the diaphragm will burst. Therefore, the diaphragm is a backup device to keep internal pressure within a stipulated limit. Other examples include blowout panels to prevent severe damage from dust explosions or safety diaphragms in missile motors to relieve overpressures caused by cracked or otherwise defective propellant. Some large missile motors initially have safety diaphragms in the combustion chamber opposite the nozzle for safety prior to launch. If ignition should occur when the motor is in storage prior to assembly, the burned gases would rupture the safety diaphragm and discharge through both the diaphragm and exhaust nozzle. Because gases are expelled in both directions, the motor will remain relatively stationary. When the missile is assembled for firing, the diaphragm is covered. Another type of pressure weak link is the freeze plug in vehicle engines. To avoid damage to cylinder blocks due to the freezing of water, metal plugs are incorporated at strategic points in the outside of the cooling system. When the water drops to the temperature at which it expands prior to freezing, the plugs are pushed out and prevent damage to the cylinder block.

4. *Structural.* A fourth type of weak link is a structural type. A component is designed with reduced strength so that it will fail at a specific point or along a specific line. A common example is the shear pin in drive couplings. The shear pin is designed to fail under excessive loads that could damage either the driving or driven equipment by the continued application of force. Structural weak links have been proposed as crashworthiness features of aircraft and helicopters. The fuselage would be designed to fail along certain lines and open up in the event of a crash. This would provide means whereby the crews and passengers could escape or be rescued rapidly and could avoid being trapped in a fire.

In each of the examples cited, the weak links have one critical, inherent fault—the equipment in which the fault was incorporated could not be operated again until the weak link had been replaced. To overcome this drawback, nondestruct safety devices have been developed. Examples follow:

1. Circuit breakers open when currents exceed set limitations and then reclose when they are within limits so the equipment can operate again.

2. Army light aircraft and helicopter engine lubrication systems may be equipped with a type of thermally activated safety device that operates at both temperature extremes. In very cold environments, the congealed oil cannot flow through the oil cooler at all. In this instance, the thermal safety device opens a bypass around the oil cooler to prevent pressure buildups that could damage it. When the temperature is very hot, all of the circulating oil should move through the oil cooler, and the cooling air inlets to the oil cooler should be fully open. Now the thermal bypass valve is in the fully closed position and forces all the oil to pass through the cooler. In addition, the thermal safety device opens the air inlets in the event that the automatic control is malfunctioning and has not opened the inlets.

Weak links also are used in conjunction with nondestruct devices, but as secondary or ultimate safeguards. Thus a relief valve on a pressure vessel takes care of temporary and minor excesses of pressure. If the relief valve becomes inoperative or has inadequate capacity, a weak link diaphragm then protects against a violent pressure vessel rupture.

9-2.13 SAFE TEST CONSIDERATIONS

The methods presented previously in this chapter have fallen into two principal categories: (1) methods intended to eliminate or reduce the possibilities of accidents and (2) methods intended to contain and minimize the damage and injuries that could result should accidents occur. There are other situations, however, when the distinction between the two categories is not so clear-cut. One of these is the testing of prototypes as distinguished from routine production, quality control, or maintenance testing. Another is "faulty-hardware" testing.

When a prototype is tested to failure or to determine the adverse influences of an environmental factor, the damage incurred cannot be considered the result of an accident. Still, the effects of the failure or environmental factor must be controlled to minimize any damage and to prevent injury to personnel. To complicate matters, the prototype testing may require the development of means to eliminate or minimize hazards that have not been encountered previously and are not fully understood. During prototype testing there are numerous uncertainties to be considered regarding hazards, for example.

1. Were the hazards that could be present during prototype testing considered during design or analysis of the system?

2. Were the ways considered whereby control of hazards could be lost?

3. Will the accident or damage control measures that were incorporated into the equipment or test facilities be adequate?

4. Could the effects of an accident or of a test failure be more severe than expected so that the safeguards against damage or injury would be overwhelmed?

5. Will the first failure occur sooner, or will the frequency of failure be greater than expected?

Thus the prototype testing must be considered almost the same as a contingency and be conducted with the understanding that there is high probability of an accident. The chief difference between the two is that a contingency is generally unexpected, whereas an adverse event resulting from a prototype test is not unexpected. Thorough preparations can be taken to minimize the damage that could possibly result from a test. All foreseeable protective equipment and arrangements can be provided and made ready before the test is begun. In many cases, the system or equipment is thoroughly instrumented so that programmed conditions or events can sometimes be detected immediately and the test can be interrupted before an unexpected accident can develop.

If the prototype is to be tested to failure, the test must be conducted with minimal possibility of an accident and with minimal damage resulting from an accident. This will require that procedure and contingency analyses be conducted as described in Chapter 8. Whenever loss of control of a hazard or damage could occur during a programmed test, the optimal accident prevention and loss containment measures of this chapter should be followed.

The need for augmented accident prevention and loss containment measures is especially important in tests to evaluate the effects of an abnormal condition, such as double charge of propellant in an artillery piece or for "faulty-hardware" testing. Faulty-hardware testing (Ref. 29) is undertaken to determine the causes of excessive failure rates of production items. Fig. 9-12 indicates the program concept for conducting faulty-hardware testing. The figure shows, via a procedure flow manner, the steps in a faulty-hardware testing program. This sample program covers all types of ammunition and subsystems containing solid or liquid fuel.

The same approach can be used for any safety-critical equipment or subassemblies. As the steps in the sample flow program are accomplished, each deliberate fault will produce certain effects that are identified in the analysis and testing process.
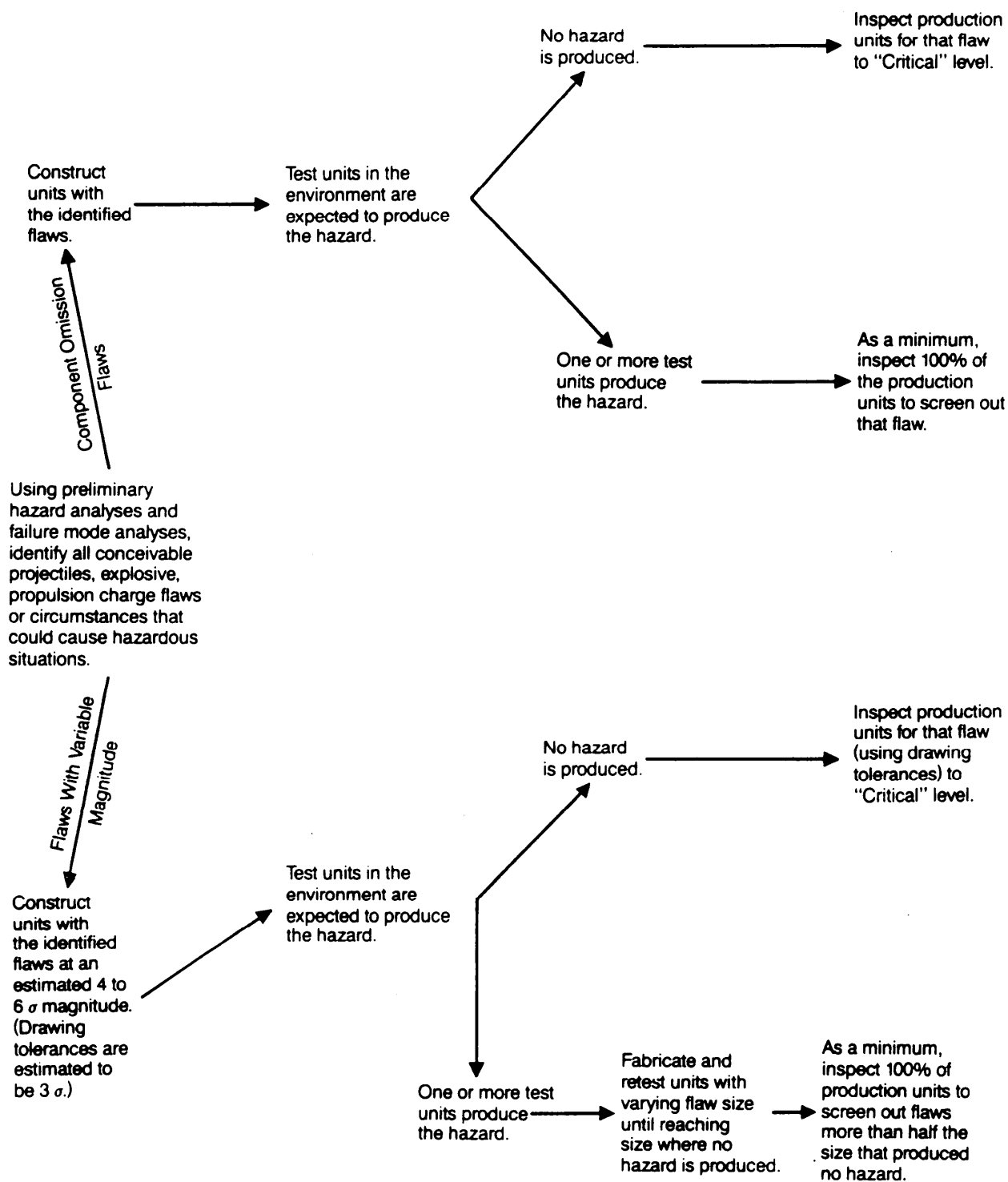
No hazard
is produced.

Inspect production
units for that flaw
to "Critical" level.

Construct
units with
the identified
flaws.

Test units in the
environment are
expected to produce
the hazard.

One or more test
units produce
the hazard.

As a minimum,
inspect 100% of
the production
units to screen out
that flaw.

Component Omission Flaws

Using preliminary
hazard analyses and
failure mode analyses,
identify all conceivable
projectiles, explosive,
propulsion charge flaws
or circumstances that
could cause hazardous
situations.

Flaws With Variable Magnitude

No hazard
is produced.

Inspect production
units for that flaw
(using drawing
tolerances) to
"Critical" level.

Construct
units with
the identified
flaws at an
estimated 4 to
6 σ magnitude.
(Drawing
tolerances are
estimated to
be 3 σ.)

Test units in the
environment are
expected to produce
the hazard.

One or more test
units produce
the hazard.

Fabricate and
retest units with
varying flaw size
until reaching
size where no
hazard is produced.

As a minimum,
inspect 100% of
production units to
screen out flaws
more than half the
size that produced
no hazard.

Figure 9-12.   Sample Faulty-Unit Plan Flow Diagram (Ref. 29)

In the sample program of Fig. 9-12, the unit to be tested could be a safing and arming (S&A) device for a high-explosive warhead. If the interruptor is left out of the S&A device, the test may indicate insufficient protection against accidental firing of the warhead. Therefore, the last step—100% inspection—may be the only reasonable insurance against the possibility of the interruptor's being omitted in assembly of the S&A device. Ref. 29 also indicates (Fig. 9-13) that the probability of at least one failure during the testing increases with the number of
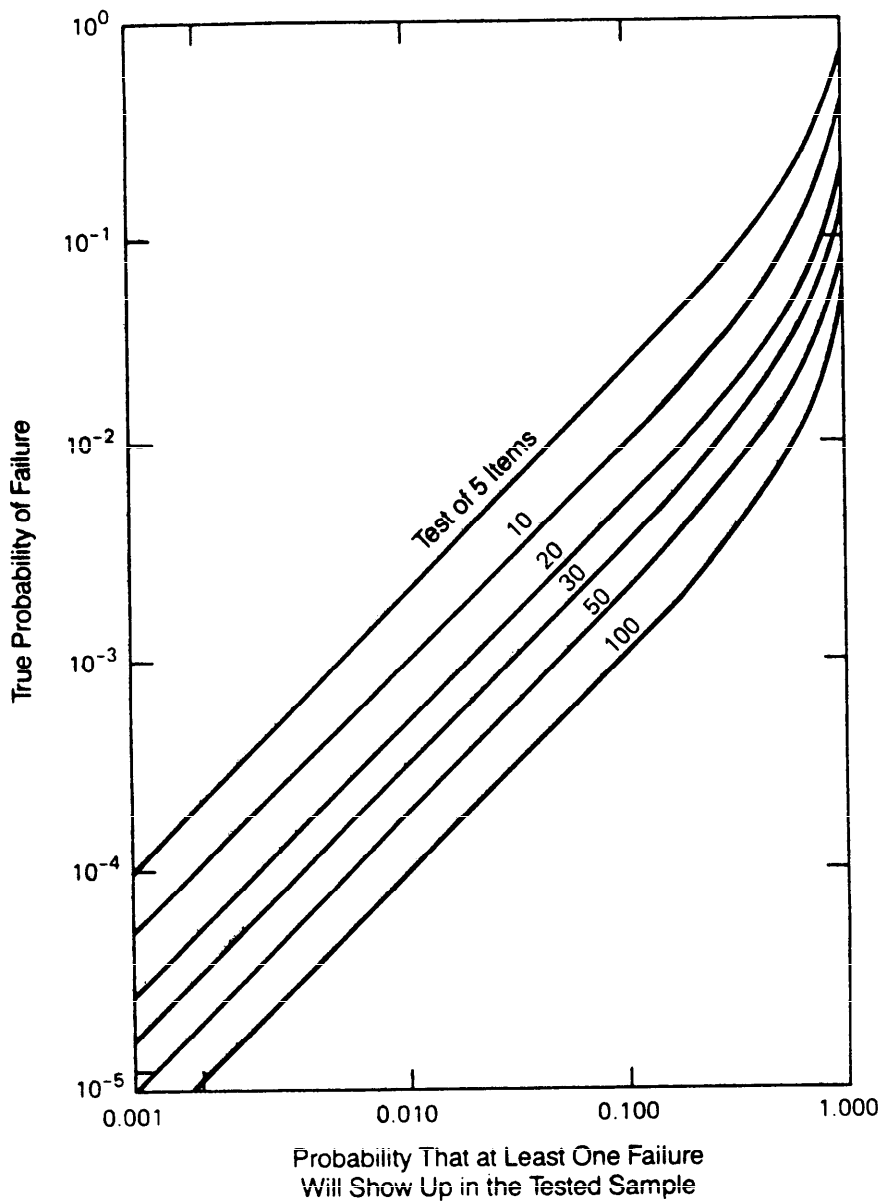
Figure 9-13. Relationship Between Real Probability of Failure and Likelihood of Experiencing Failure in Testing Various Numbers of Items (Ref. 29)

tests conducted. With the increased probability of a failure and an accident, the need for loss control increases.

Accidents with Army equipment in field use are low-probability events, but they generally occur at highly inconvenient times; they usually disrupt operations and can be as devastatingly damaging as enemy action. Prototype and faulty-hardware testing will develop information that can reduce both the occurrences of the accidents and the magnitudes of the resultant damage. To accomplish this, the information derived from the tests must be

provided to the personnel and organizations responsible for taking corrective action. (The results of Army tests of new weapons are categorized in accordance with Ref. 30.) The testing of Army materiel is planned, conducted, and monitored by the materiel developer—in most cases the US Army Materiel Command (AMC). The US Army Test and Evaluation Command (TECOM) manages testing and operates the Army proving grounds and test centers. Accordingly, TECOM should be consulted for safe test procedures and considerations.

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

2. MIL-STD-454J, *Standard General Requirements for Electronic Equipment*, 26 February 1987.

3. MIL-STD-1472C, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities*, 17 March 1987.

4. MIL-P-5518C, *Pneumatic Systems, Aircraft, Design, Installation and Data Requirements for*, 9 July 1962.

5. W. Hammer, *Product Safety Management and Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

6. National Fire Code No. 493, *Intrinsically Safe Apparatus*, Chapter 2, National Fire Protection Association, Boston, MA, 1978.

7. M. Halebsky, *Intrinsic Safety—Qualitative and Quantitative Aspects*, (company paper) Litton Ship Systems, Culver City, CA, April 1972.

8. W. F. Hickes, "Intrinsic Safety and the CPI", *Chemical Engineering Progress*, 67-74 (April 1968).

9. W. A. Power, "An Intrinsic Safety Primer", *Instruments and Control Systems*, 99-100 (September 1971).

10. AMCP 706-196, Engineering Design Handbook, *Development Guide for Reliability, Part Two, Design for Reliability*, January 1976.

11. AMCP 706-197, Engineering Design Handbook, *Development Guide for Reliability, Part Three, Reliability Prediction*, January 1976.

12. AMCP 706-198, Engineering Design Handbook, *Development Guide for Reliability, Part Four, Reliability Measurement*, January 1976.

13. AMCP 706-200, Engineering Design Handbook, *Development Guide for Reliability, Part Six, Mathematical Appendix and Glossary*, January 1976.

14. F. R. Taylor, *Impact of Reliability Requirements on Flight Control Development*, Air Force Flight Dynamics Laboratory, Wright-Patterson AFB, OH, March 1967.

15. M. Longden, L. J. Page, and R. A. Scantlbury, "An Assessment of the Value of Triplicated Redundancy in Digital Systems", *Microelectronics and Reliability*, Pergamon Press, London, England, 1966, 39-55.

16. AR 750-22, *Army Oil Analysis Program*, 12 April 1977.

17. G. E. Muller and C. J. Schmid, *Factor of Safety—US Air Force Design Practice*, AGARD Report No. 661, Air Force Flight Dynamics Laboratory, Wright-Patterson Air Force Base, OH, November 1977.

18. ANSI Z35.1-72, *Specifications for Accident Prevention Signs*, American National Standards Institute, New York, NY, 1972.

19. ANSI C95.2-66, *Radio Frequency Radiation Hazard Warning Symbol*, American National Standards Institute, New York, NY, 1966.

20. MIL-M-38784B, *Manual Technical, General Style and Format Requirements*, 16 April 1983.

21. *Code of Federal Regulations*, Title 21, "Food and Drugs", 1 April 1975.

22. MIL-STD-101B, *Color Code for Pipelines and for Compressed Gas Cylinders*, 3 December 1970.

23. MIL-STD-1247B, *Markings, Functions and Hazard Designators of Hose, Pipe, and Tube Lines for Aircraft, Missile, and Space Systems*, 20 December 1968.

24. *Product Safety Sign and Label System*, FMC Corporation, Santa Clara, CA, January 1980.

25. *Agricultural Yearbook*, American Society of Agricultural Engineers, St. Joseph, MI, 1975, 291-2.

26. "Signs of the Times", *Dimensions*, National Bureau of Standards, Washington, DC, March 1980, 2-6.

27. H. Dreyfuss, *Symbol Sourcebook*, McGraw-Hill Book Company, New York, NY, 1972.

28. DARCOM-P 706-298, Engineering Design Handbook, *Rocket and Missile Container Engineering Guide*, January 1982.

29. J. S. Nerrie, *Underlying Concepts and Assumptions for Faulty-Hardware Safety Testing*, Report TR-3478, Naval Surface Weapons Center, Dahlgren, VA, August 1976.

30. *Classification of Deficiencies and Shortcomings*, TOP-1-1-012, US Army Test and Evaluation Command, Aberdeen Proving Ground, MD, April 1979.

BIBLIOGRAPHY

R. J. Will, "Selecting Speed Reducers", *Machine Design*, 116-20 (September 1977).

CHAPTER 10
HAZARDS

This chapter categorizes hazards according to their origins and the effects they can generate. Fifteen hazards are discussed in detail. The text presents information from the literature on human tolerance and safe exposure limits for each hazard; references are provided for more exhaustive detail. Direct and indirect sources of each hazard are addressed. Examples of design techniques illustrate ways to eliminate or control these hazards or, as a last resort, to provide effective warnings. This information can be used in conjunction with the methods described in Chapter 9 to avoid or reduce the possibilities or probabilities of an accident or to minimize injuries and damage from accidents.

10-1 INTRODUCTION

MIL-STD-882B (par. 3.1.3) (Ref. 1) defines a hazard as "A condition that is prerequisite to a mishap.".

For years, the safety levels of systems were improved haphazardly, i.e., by eliminating and controlling those hazards that were readily apparent to designers. Now, however, system safety engineers and analysts are concerned with making these improvements systematically so that *all* potential hazards—apparent and hidden—are identified, analyzed, and subjected to suitable safeguards. The paragraphs that follow describe how this chapter is organized to discuss hazards and their remedies systematically.

Studies have shown that hazards can be grouped in a number of ways. One method—the one used in this chapter—is to group hazards by major categories of physical phenomena. Under each major category the related conditions, energy sources, and the properties or states of the hardware of the system are considered. The categories of physical phenomena are then presented in an order (See Table 10-1.) to enable the sequencing of hazards such that related information on other hazards readily follows. For example, thermal hazards are discussed early so that the effects of heat on pressure hazards can later be discussed without repetition. For the same reason, basic information on chemical reactions is presented before phenomena of contamination, material deterioration, and fire and explosion—all of which are chemical reactions.

Table 10-1 lists 15 major hazard classes of physical phenomena and identifies the subclasses of hazards included in each. The table is in the form of a checklist. It can be used by designers or analysts to review systems, subsystems, assemblies, components, tasks, or operations for hazards. The designer enters each component of the system, equipment, tasks, or operation at the top of the table and designates it by a letter—A, B, C, D, etc. In an electric power subsystem, the battery might be A, the

generator B, the voltage regulator C, the reverse current relay D, etc. Each hazard in the list is considered and evaluated against the item heading each column. If the relationship bears investigating, the analyst marks the column and line. On a separate sheet of paper, the analyst lists the column letter and line number and adds comments. This information can provide the basis for a preliminary hazard analysis or a system or subsystem hazard analysis.

Experience and theoretical considerations have shown that, with certain types of equipment or operations, some of the subcategories of hazards can be eliminated immediately and need not be considered. For example, under the "electrical" category it is unnecessary to consider the subcategories of electrical shock or fires if the equipment under study operates only with low voltages except under specifically adverse conditions.

The format for the treatment of each hazard class is
1. Discussion of hazard
2. Tolerance and safe exposure limits
3. Potential hazard sources
4. Safety criteria for designers to follow.

10-2 ENVIRONMENT

In a safety analysis of a system, one of the first considerations is the adverse effects that outside conditions can impose on the system. These outside conditions constitute the environment—the totality of natural and induced conditions occurring or encountered at any one time or place—in which the system will exist and operate. Refs. 2 and 3 present detailed discussions on natural and induced environments, respectively. Induced environmental factors are those for which man's activities constitute the major contribution relative to the effects of these factors on personnel and materiel. They may be similar to natural environments, with such modifications as elevated or lowered temperatures and or humidities, or they may be alien environments (vacuum, inert gas, etc.). The various

TABLE 10-1. HAZARD CLASSES

Hazard Classes (of Physical Phenomena) With Subclasses	A	B	C	D	E	F

1. Environment
   Lightning
   Heat
   Rain
   Snow
   Wind						

2. Thermal
   Heat
   Cold
   Solar
   Changes
     Wind factor						

3. Pressure
   Pneumatic
   Hydraulic
   Changes
     Hot-Cold (in closed container)						

4. Toxicity
   Systemic
   Asphyxiants
   Irritants
   Gaseous
   Liquid-Solid						

5. Vibration
   High Frequency
   Low Frequency
   Transmission
   Induced						

6. Noise
   Intensity
   Duration						

7. Radiation
   Frequency
   Ionizing
     X rays
     Alpha particles
     Beta particles
     Gamma rays
     Neutrons
   Nonionizing
     Ultraviolet
     Infrared
     Microwave
     Laser						

Hazard Classes (of Physical Phenomena) With Subclasses	A	B	C	D	E	F

8. Chemical Reactions
   Corrosion
   Combinations
   Dissociations
   Replacement						

9. Contamination
   Combination
   Foreign Substance
   Fungal Growth
   Dissociations						

10. Material Deterioration
   Stress
   Aging
   Wear
   Environment
   Fatigue						

11. Fire
   Fuels
   Oxidizers
   Ignition Sources						

12. Explosions
   Sensitivity
   Low Order
   High Order
   Fragmentation						

13. Electrical
   Shock
   Fire
   Heat
   Explosions
   Static						

14. Acceleration
   Mass
   Time
   Secondary						

15. Mechanical
   Stability
   Sharp Edges
   Moving Parts
   Tolerances						

environmental factors and their effects on materiel and personnel are described briefly in this paragraph. Those factors that represent significant hazards are discussed in detail in pars. 10-3 through 10-16.

The natural environment generally is considered to be those climatological and meteorological conditions that occur without man-made changes or effects. Elements of the natural environment that must be considered in safety analyses include solar radiation, temperature, rain and humidity, pressure, dust and sand, snow, wind, ice, hail, fog, and combinations of these. Ref. 4 investigates other environmental influences—such as magnetic, lunar, and solar influences; barometric pressure; and time of day and annual cycles—that could influence persons to cause accidents. These natural elements may generate adverse effects even when not at either extreme of their limits.

Fig. 10-1 (Ref. 5) indicates some zones of comfort and discomfort for humans subjected to both natural and induced environmental effects in air travel. Combinations of environmental effects from the discomfort zone—e.g., high temperature, noise, acceleration and pressure change—will increase the degree of discomfort. When these environments are encountered, the data of Fig. 10-1 can be used as a guide to provide an indication of the degree of severity at which the environment must be controlled or modified by design for operators who must maintain their concentration in military task performance. Other limitations for various hazards are given later in this chapter.

Environmental limits for equipment are generally stipulated in the equipment specifications. Determination of what limits to impose in the equipment specification can be obtained from such Government groups and their publications as The National Council on Radiation Protection, Occupational Safety and Health Administration regulations, the American Conference of Governmental Industrial Hygienists, the National Institute of Occupational Safety and Health, and military standards—such as 1474 (Ref. 6), 1472 (Ref. 7), and 454 (Ref. 8)—which apply to the specific areas of audio noise, human engineering, and electronic equipment, respectively. The TB MED series of military bulletins also contains guidance for control of hazards, e.g., TB MED 524 (Ref. 9) covers the hazard control criteria for laser devices.

Verification that designs meet imposed limitations is accomplished by methods indicated in MIL-STD-810 (Ref. 10). Each method listed in the standard covers a specific topic of testing. For example, Method 508.2 covers testing for fungus to insure that the specification requirement for resistance to fungous growth has been met. Since each topic is a thorough treatment of the test method for that topic alone, the standard is quite lengthy. The designer should have access to this document within his parent Army organization.

Not only is Army equipment susceptible to the natural environment, but it may also contribute adversely to the

natural environment. Modifying the natural or man-made environment so that Army personnel can achieve optimum performance is covered in par. 5.8, MIL-STD-1472 (Ref. 7). This guidance includes criteria for heating, ventilating, air conditioning, illuminating, acoustical noise, and vibration. The graphs and tables of environmental requirements and data will provide designers of Army equipment with considerable environmental background information.

Par. 5, MIL-STD-1474 (Ref. 6), covers criteria relating to the audio noise environment. Table 4 of this standard, reproduced here as Table 10-2, provides some quick reference information on sound-level requirements.
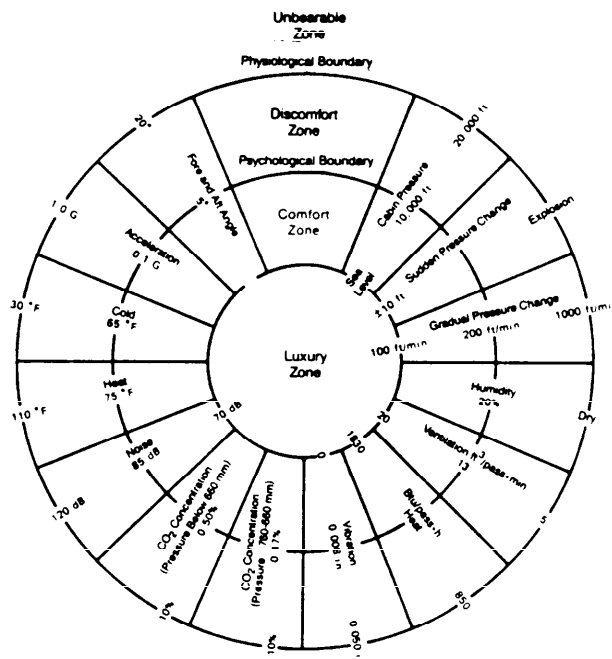
Table of Conversion

0.05 in. = 0.00137 m = 1.37×10^{-3} m
0.008 in. = 0.0002032 m = 2.032×10^{-4} m
65°F = 18.33°C
30°F = -1.11°C
75°F = 23.89°C
110°F = 43.33°C
100 ft/min = 0.508 m/s
200 ft/min = 1.016 m/s
1000 ft/min = 5.08 m/s
ft^3/pass·min = 4.719×10^{-4} m/pass·s
10 ft = 3.048 m
10,000 ft = 3048 m
20,000 ft = 6096 m
Btu/pass·h = 2.931×10^{-1} W/pass

From *Human Factors in Air Transportation* by R. A. McFarland, McGraw-Hill Book Company, New York, NY, 1953.

Figure 10-1. Zones of Luxury, Comfort, and Discomfort for Humans (Ref. 5)

TABLE 10-2. SOUND LEVEL LIMITS AND TEST PROCEDURES
FOR EXTERIOR NOISE (Ref. 6)

Type of Equipment	Gross Weight or Capacity	Distance from Centerline, m (ft)	Sound Level Limit, dB(A)[a]	Test Procedure
Motor Vehicle[b]	>4536 kg (10,000 lb)	15.2 (50)	83	SAE J366
	≤4536 kg (10,000 lb)	15.2 (50)	83	SAE J986
Construction and Material Handling Equipment			88	SAE J88
Mobile Generator[c] Sets	≤60 kW (80 HP)	7 (23)	80	SAE J1074
	>60 kW (80 HP)	7 (23)	85	SAE J1074
Portable Air Compressors for Construction Equipment		7 (23)	76	40 CFR 204

[a]See par. 10-7 for a discussion of the unit dB(A).
[b]For equipment wider than 2.74 m (9 ft), the 15.2-m (50-ft) distance shall be measured from the side of the vehicle closest to the microphone.
[c]Mobile generator sets shall be measured at governed speed and rated load at a distance of 7.0 m (23 ft) from major surfaces.

A great number of natural conditions can generate catastrophic effects that should be considered in safety analyses. These extraordinary conditions include lightning strikes, hurricanes (or similar storms), tornadoes, blizzards, floods, and earthquakes. The global use of Army equipment often requires it to be capable of surviving storms, lightning strikes, severe snowfall, and intense rainfall. Other events such as earthquakes, tornadoes, and floods are localized events, which may occur in certain geographical areas but only rarely in other areas. Survival in earthquake areas is affected by the random and unpredictable nature of the phenomenon. Generally, the more rugged the equipment, the better its chances for survival in an earthquake.

Induced environments include the following:

1. All natural environments that have been affected by human action—e.g., locally elevated temperatures resulting from a chemical process; air laden with dust created by vehicles, mining, farming, or combustion of coal; or vibration caused by the passage of aircraft, trains, or other ground vehicles.

2. Controlled environments, which are natural environments that have been modified in some respect to mitigate or avoid an adverse condition of the natural environment. Air-conditioning to reduce temperature and humidity is an example of modifying the natural environment.

3. Any artificial environment, one that is totally different from the natural environment by which the equipment or system is surrounded. An example is nitrogen or other inert gas in enclosed compartments to prevent fires that might occur if air were present.

In combat situations, induced environments must also include the conditions created through nuclear, biological, and chemical (NBC) elements of warfare. Each of these elements is a specialized subject whose technical characteristics will not be described here. However, the effects of these elements in contaminating Army equipment—and the subsequent decontaminating—must be considered in the system design process. Certain design features are readily susceptible to this type of contamination and should be avoided. Other design features can increase the effectiveness of the decontamination process, and they should be emphasized.

In general, any external—or internal if the equipment is not completely enclosed—design feature that can trap or retain a solid, liquid, or gaseous material represents poor design with respect to contamination and decontamination. Such features not only tend to hold contaminants—and thus represent potential personnel hazards—but they are difficult to clean adequately. Guidelines that facilitate decontamination follow (Ref. 11):

1. Lapped surfaces typical of sheet metal panels, cabinet walls and doors, compartment covers, and deck plating—particularly if joined by bolts or rivets—lead to conditions that can trap contaminants and make decon-

tamination extremely difficult. Welding is the preferred method of joining. If rivets, bolts, or screws are used, contaminants can be drawn into the capillary under the fastener heads. Accordingly, the seams, cracks, and crevices presented by lapped surfaces and fasteners must be sealed by a nonabsorbant paint or strippable sealing compound.

2. Concave surfaces that can trap liquids and solids during runoff should be avoided unless the concavity serves a useful function, e.g., a bullet deflector. Otherwise, the entrapment areas should be filled, rounded so water will run off, or provided with holes for runoff with no entrapment in the drains.

Possible decontamination troublespots requiring special design attention are toolboxes and their mountings; ballistic gratings, doors, and hatches; lighting installations; lap joints; vision blocks; antenna mountings; gun gas evacuators; track wheels; tool and equipment mountings on vehicles; and chain and/or cable storage.

For individual pieces of equipment, an acceptable decontamination solution is the provision of shrouds that completely cover the piece but permit operation. If rolling and sliding bushings and bearings cannot be covered or shielded, special seals will be required.

The designer should note that many solutions to the contamination problem involve the correct development of geometric shapes and methods of fastening in the design phase. Once the hardware has been designed and built, generally, there are no easy methods to correct design deficiencies in the area (or, for that matter, in most other safety areas either). Ref. 11 contains information to assist the designer in understanding the NBC contamination problem and designing solutions for it.

All controlled and artificial environments must exist in limited spaces and, therefore, constitute "closed" environments. Closed environments can also be those that simply protect against the natural environment without otherwise modifying it. An example is a building, which protects against rain or wind. A "free" environment poses no interference to the movement of air. Such unrestricted movement, however, may permit the introduction of undesirable agents, such as dust or dirt into an engine, into a local environment. In some situations, the closed environment may be far more dangerous than a free one. The spillage of a small amount of a toxic chemical could be of minor consequence in a free environment but deadly in a closed one.

Thus it is apparent that environmental hazards include not only those meteorological and climatological conditions of the natural environment but also those conditions resulting from induced environments generated by humans. In both types of environments, similar conditions will generate similar effects. Therefore, both types of environments can be assessed for hazards in the same

manner. Table 10-3 (Ref. 12) indicates some of the environmental hazards and their causes.

In the natural environment, temperature is probably the most common hazard to equipment and personnel. The low temperatures commonly experienced in the winter months in the majority of the land areas of the United States are sufficiently severe to cause damage to unprotected liquid-cooled vehicles. Without antifreeze protection, the liquid in the engine cooling system would freeze and rupture the block if it were not for freeze plugs in the wall of the engine. Extremely low temperatures also affect rubber hoses, electrical insulation, drive belts, etc., and cause failures.

Ice on the surface of streets causes many accidents each year. To make matters worse, the salt used to overcome this road hazard causes much damage to the metal parts of vehicles and thus creates still another hazard.

In induced environments high temperatures often cause problems. During normal operations equipment often generates heat that causes electronic components to fail more quickly. High temperature can also make existence in closed spaces unbearable for the occupants.

Moisture is another common hazard of the natural environment. It causes rust on metal parts; expansion of nonmetallic materials with consequential mechanical binding; and shorting of electrical equipment. Moisture also can adversely affect the performance of personnel.

Temperature variations can either increase or decrease the effect of moisture in causing rust and corrosion. The combination of high humidity and changes in temperature will cause condensation and collection of moisture in unwanted locations such as fuel tanks. Rain can cause damage to equipment in much the same way as humidity. Additionally, rain can wash paint and lubrication from surfaces and can collect in low places, which increases weight and causes overstress. Fog can limit visibility and mission accomplishment.

Wind is a hazard primarily during thunderstorms and in certain geographical locations. Army equipment must be designed to withstand wind effects. Vehicles must be protected against overturning, engines must be protected against blown dirt and dust, and all types of equipment must be protected against wind-borne debris, which can behave like missiles. Winds in mountainous areas are hazardous to low-flying aircraft. In winds exceeding 5.14 m/s (10 kn) helicopters must be operated cautiously, especially when starting and stopping the rotors.

Dust, sand, and other solid particulate matter can cause severe damage to unprotected equipment. Wind-borne solids have stripped paint off Army vehicles, roughened glass, clogged oil and air filters and systems, and caused internal, abrasive damage to inadequately protected moving parts. Pollutants cause eye and lung irritation and corrosion hazards.

TABLE 10-3. ENVIRONMENT AND WEATHER CAUSES, AND POSSIBLE EFFECTS ON EQUIPMENT AND PERSONNEL (Adapted from Ref. 12)

Causes	Possible Effects on Equipment	Possible Effects on Personnel
Heavy Rain, Floods, High Humidity Rain, clouds, fog, dew, snow Tides and floods Lakes, rivers, and other natural water sources Vegetation and animal respiration Temperature decrease without removal of moisture Condensation on cold surfaces Flooding and immersion in water Naturally high atmospheric humidity Personnel perspiring in inadequately ventilated enclosure, equipment, or impermeable covering Presence of humidifying equipment	Loss of visibility due to fog, clouds, or condensation Possibility of acceleration of corrosion Short circuits, inadvertent activations, or disruptions of electrical systems by moisture condensation in electrical devices Surface friction for traction reduced by wet surfaces Skidding and loss of control of vehicle caused by wet surfaces Swelling of water absorbent materials Warping and sticking of wood doors, drawers, and similar items	Deterioration of general health under prolonged exposure Reduced efficiency in operations requiring skill Induced errors in tasks requiring high concentration
Low Humidity Hot weather with little moisture Heat in a closed room in winter Moisture removed by air-conditioning	Drying out and cracking of organic materials Generating dusty conditions Increased tendency for creation of static electricity Easier ignition of accidental fires Increase in airborne salts, sand, dirt and fungi	Skin chapped and nasal areas dried Slight discomfort for normally healthy people
Sunlight	Ultraviolet radiation effects of sunlight Infrared radiation effects	Eye strain and/or burn Sunburned skin where unprotected Snow blindness Difficulty in guiding a vehicle or in reading dials and meters caused by strong sunlight
Meteorological and Micrometeorological Conditions Wind Hail Heavy Rain	Flooding Filling floating vehicles with water Washing away equipment Structural overloads, movement, or toppling caused by pressure effects of wind Sudden accelerations due to turbulence and gusts of wind Energized power lines blown down by wind Impact damage caused by hail	Shock from downed power lines Physical injury from windblown debris Physical injury from large hailstones Drowning of personnel

TABLE 10-3 (cont'd)

Causes	Possible Effects on Equipment	Possible Effects on Personnel
Lightning and Thunder Electromagnetic interference with electronic equipment not adequately shielded	Initiates or activates electrical devices in path of lightning discharge or in proximity of electromagnetic pulse or electric field Overloading of electrical circuits and equipment Ignition of combustible materials	Shock to personnel
High and Low Pressure Water pressure, atmospheric pressure Reduced atmospheric pressure Changes in pressure	Air-breathing engines affected by changes in atmospheric pressure Implosions and crushing of closed vessels Pressure vessel ruptures	Dysbarism and bends in humans Reduced physical capability at low atmospheric pressure (equivalent to 3048 m (10,000 ft) and above)
High Temperature Summer heat Tropical heat Heat from engines Heat from chemical processors and reactions Body heat Welding Friction	Melting of metals and sealants Fires or conditions that permit easy vaporization Rapid evaporation of liquids Reduced reliability of electronic equipment Loss of lubricating effects Increased gas pressure	Skin burns Heat exhaustion, heat prostration Loss of ability of persons to function
Low Temperature Winter cold Arctic and antarctic conditions High altitudes Refrigerated surfaces Cryogenic lines and equipment	Plastics and metals become brittle Lubricants congeal Freezing of liquids Failure of engines and thermal processes	Inefficient performance on tasks requiring dexterity (Protective clothing also interferes with performance.) Cold "burns" Frostbite, chilblains
Airborne Salts, Dusts, Sand, and Dirt . . . Desert and beach areas Dry areas subject to much traffic Sandstorms Windblown dust, dirt and other solid matter Salt used to melt ice on roads Marine environment	Contamination by salt, sand, dirt, moisture, fungi Concentration of toxic gases, smog, or particulate matter caused by inversions Electrical conductivity of water increased by salt, which reduces insulation value and permits galvanic coupling and deterioration of adjacent dissimilar metals	Causes respiratory ailments to develop Restricts visibility Injures eyes

Snow can cover air inlets and clog air filters. In wet, freezing weather snow will stick to glass surfaces and interfere with visual observation. On the ground, snow can trap vehicles or prevent adequate traction, which leads to immobile or uncontrollable vehicles.

Some design solutions to the discussed environmental problems include

1. Providing filters of appropriate size and type for air-breathing engines and for personnel air ventilation subsystems

2. Applying abrasion- and corrosion-resistant coatings to the outer surfaces of equipment

3. Providing alternate air inlets for use when normal inlets are frozen with wet snow or freezing rain

4. Providing personnel with masks to filter out or neutralize specific pollutants identified as possible hazards

5. Providing lug tires or other snow tire designs and/or chains for use in various types of low-traction operations ranging from freezing rain to deep mud.

Vibration, radiation, and electrical shock are examples of induced environments that can adversely affect the performance of humans and equipment. Vibration—depending on its frequency and amplitude—can cause annoyance, discomfort, or illness in humans. Accordingly, designs should limit whole-body vibration to levels that permit safe operation and maintenance. Equipment subjected to excessive vibration—whether induced or self-generated—can malfunction or be damaged.

Fig. 10-2 (Ref. 13) shows the maximum allowable exposure times that will maintain proficiency for different combinations of acceleration and frequency levels. For instance, the maximum exposure time for an acceleration of 0.5 m/s² and a frequency of 1.6 Hz in the longitudinal direction is 8 h (Point A). For acceleration and frequency

level combinations above the 8-h curve, exposure time must be reduced accordingly to maintain proficiency. In case of multidirectional vibration, each direction is to be evaluated independently with respect to limits presented in Fig. 10-2.

Limits on whole-body vibration to accommodate the human body follow (Ref. 13):

1. *Safety Limits.* To protect the human body, whole-body vibration should not exceed twice the acceleration values in Fig. 10-2 for the times and frequencies indicated.

2. *Proficiency Levels.* When proficiency is required for operational and maintenance tasks, whole-body vibration should not exceed the acceleration values in Fig. 10-2 for the times and frequencies indicated.

3. *Comfort Level.* Where comfort is to be maintained, the acceleration values in Fig. 10-2 for a given frequency should be divided by 3.15.

4. *Motion Sickness.* Very low-frequency vertical vibration should not exceed the limits given in Fig. 10-3 (Ref. 13) to protect 90% of the unadapted males from vomiting in the exposure time indicated.

Where both whole- and part-body vibrations are not a factor, equipment should be designed so that oscillations will not impair human performance with respect to control manipulations or the readability of numerals and letters. Such equipment should be designed to preclude vibrations in the shaded area of Fig. 10-2(A).

Vibration may be detrimental to the operator and the maintenance technician's performance of both mental and physical tasks. Large amplitude, low-frequency vibrations contribute to motion sickness, headaches, fatigue, and eyestrain, and they interfere with depth perception and the ability to read and interpret instruments. Exposure to continual, high-speed vibrations promotes worker

(A) Longitudinal Direction

(B) Transverse Direction
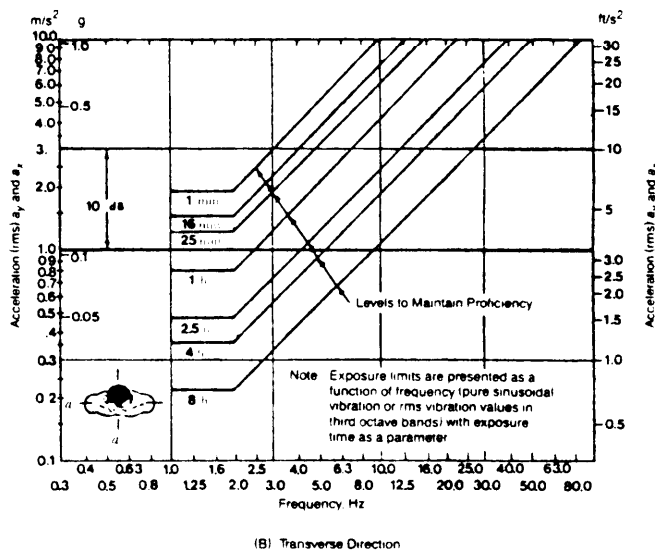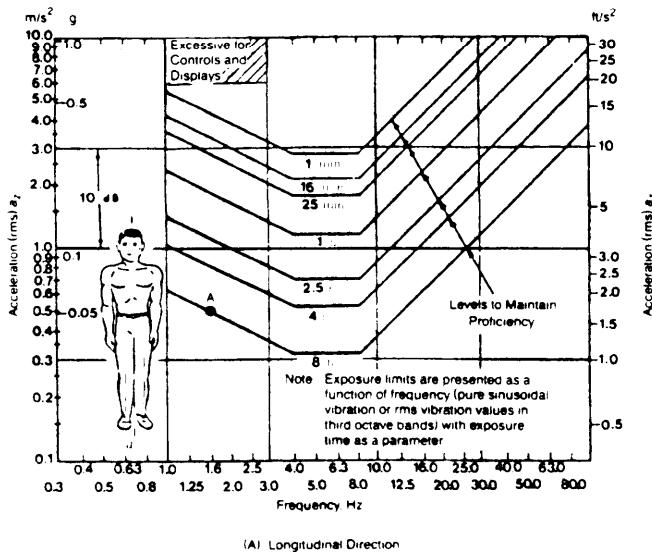
Figure 10-2. Vibration Criteria for Longitudinal and Transverse Directions With Respect to Body Axes (Ref. 13)
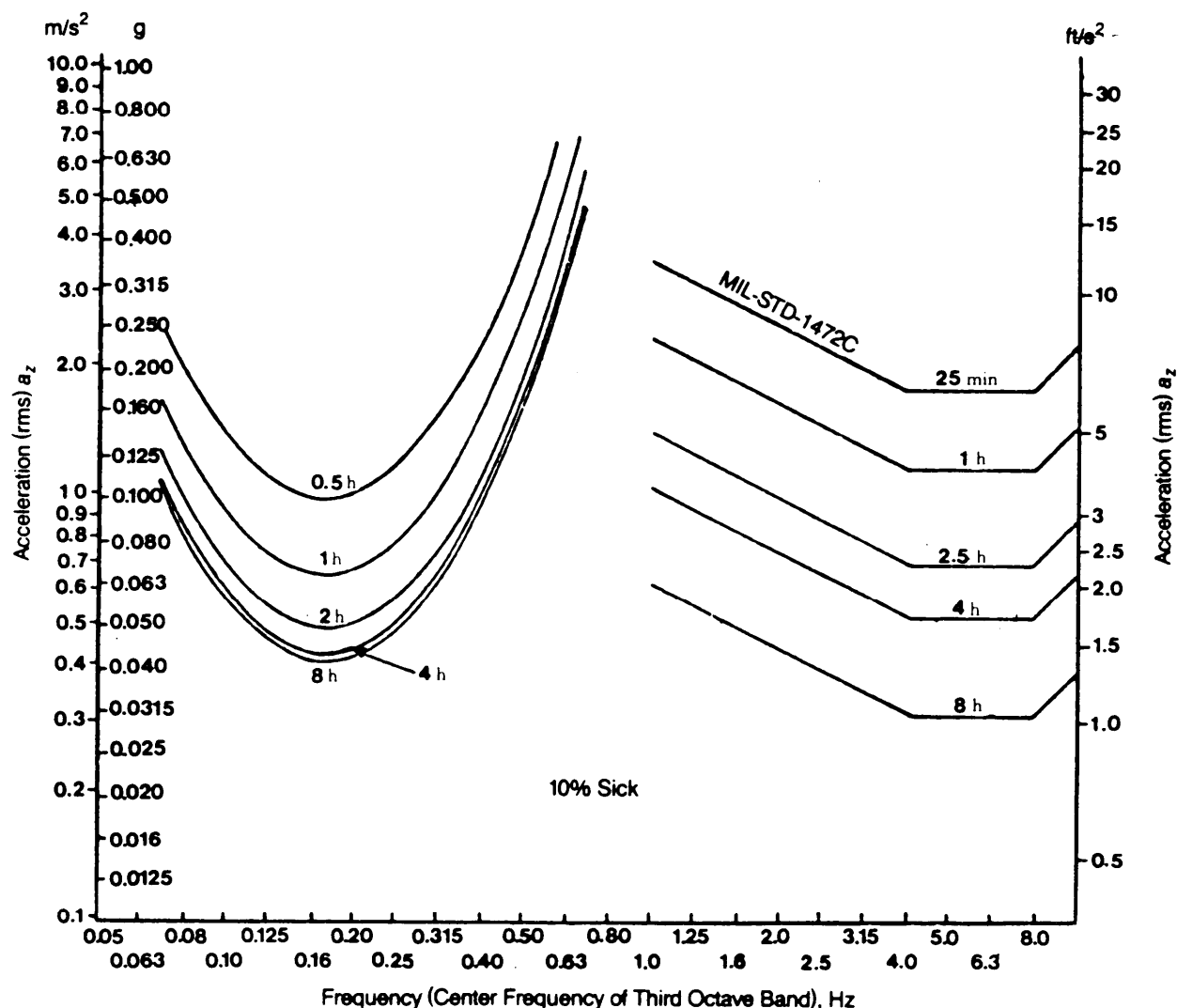
Figure 10-3. 90% Motion Sickness Protection Limits for Humans Exposed to Very Low-Frequency Vibrations (MIL-STD 1472 and ISO 2631 FDP Vibration Limits From 1 to 10 Hz Are Included) (Ref. 13)

fatigue and decreases worker proficiency. The designer can reduce and control vibration by isolation, proper balancing of rotating machinery, and provision of damping materials or cushioned seats for personnel.

Additional data to assess the effects of vibration and motion may be found in Refs. 7 and 14. A detailed discussion of vibration is presented in par. 10-6.

Another induced environmental factor to be considered is radiation. Par. 6, Requirement 1, MIL-STD-454 (Ref. 8) contains detailed hazard control criteria for both ionizing and nonionizing radiation—i.e., X ray, microwave and radio frequency, and laser. Radiation is discussed in detail in par. 10-8.

The effects of environmental hazards on human performance can be either immediate or delayed. (See Table 10-4 (Ref. 15).) The most common immediate effect is interference with operations. Material damage also may

be the result of immediate or delayed effect. Heavy rain can cause damage to electrical equipment by flooding, which shorts out circuits. Also, prolonged exposure of electrical equipment to high humidity can cause insulation to deteriorate and can result in short circuits. Much more subtle are the deleterious effects of temperature, humidity, pressure, vibration, and other environmental factors on human performance. (See Table 10-4.) There is increasing evidence that these environmental factors are highly correlated with human involvement in accidents.

Adverse effects of environmental hazards may occur independently or in conjunction. When environmental hazards act in unison, they may create effects that are totally different from the individual effects. A high temperature will accelerate corrosion in a high-moisture environment; in a lower moisture environment, its drying effect may retard corrosion. On the other hand, a low

TABLE 10-4. ADDITIVE INTERACTIONS OF COMBINED ENVIRONMENTAL STRESSES (Ref. 15)

Stresses	Test Animal	Effect	Source
Acceleration and heat	Man	Heat decreases tolerance to $+G_z$.*	Burgess
Acceleration and hypoxia	Man	Hypoxia decreases tolerance to $+G_z$.*	Burgess
Acceleration and cold	Rats	Hypothermia decreases tolerance to $+G_z$* in rats at 20 G.	Stiehm
Hypoxia and cold	Man	Cold with hypoxia increases shivering, heat production, heart rate, and respiratory ventilation.	Bullard
Hypoxia and heat	Man	Increased heart rate of 63% of 19 subjects exposed to 49°C (120°F) for 30 min at sea level, and 5500 m (18,000 ft) the last 15 min.	Hale
Hypoxia and vibration	Rats	Greater mortality in restrained rats.	Megel et al.
Hypoxia and radiation	Rats	Radiation 30 days in advance decreases tolerance to hypoxia; probably there is suppression of red blood cells from radiation injury.	Newsom and Kimeldorf
Ionizing radiation and cold	Rats	Decreased cold tolerance following neutron and X-ray radiation.	Newsom and Kimeldorf
Vibration and heat	Rats	65% mortality (26 in 40 rats exposed) when sublethal heat was combined with random vibrations (5-800 Hz, 17.5 G rms), which produces 7.5% mortality alone.	Megel et al.
Weightlessness and acceleration	Man	End point reached at lower G levels following 18 h submerged.	Benson et al.
Weightlessness, heat, and dehydration	Man	In one subject, bed rest plus heat plus dehydration of 3.6% of body weight produced a hypotensive response to 70-deg tilt.	Di Giovanni et al.

*G_z is acceleration along the longitudinal axis of the body.

temperature will generally reduce the corrosion rate, but under certain circumstances it can cause condensation, which can accelerate corrosion. Therefore, it is necessary to consider combinations of environmental factors, i.e., whether the effects are additive, synergistic, or antagonistic.

Environmental analyses must be heavily dependent on tests and experience because of the multiplicity of variations in environmental conditions that may occur. For example, although temperature and humidity are the primary factors regulating the corrosion rate, it is also affected by such factors as metal composition, heat treatment, surface finish, stress concentrations, imposed stress loading, and length and duration of vibrations. The easiest way to measure the adverse effects is to test the equipment under actual or simulated environmental conditions. Testing under actual conditions, however, is expensive and time-consuming. Therefore, any simulation technique or other process that can minimize actual testing is very cost-effective. Environmental testing of military equipment is conducted in accordance with Ref. 10. Information on safety design criteria to avoid or control corrosion is found in par. 10-9.

10-2.1 TOLERANCE AND SAFE EXPOSURE LIMITS

Human tolerance and safe exposure limits can differ greatly. Human tolerance limits determined by laboratory tests under controlled conditions show that even under exactly the same conditions, subjects will have different tolerances. For example, in air-conditioned environments where almost all persons are comfortable,

there will always be 3 to 5% who are uncomfortable (Ref. 15). Also, tolerance limits will vary with acclimation and the numerous personal preferences of the subjects.

Combinations of environmental factors make determinations of acceptable tolerance limits even more uncertain. Examination of Table 10-4 will provide insight into the effect of more than one environmental condition imposed on the human body. Some of the experiments indicate as many as three simultaneous environmental conditions imposed on the subject and the resultant changes in resistance to body orientation. In another example, ionizing radiation acts to decrease a person's resistance to hypoxia if his air intake is subsequently decreased.

In addition to the table of deleterious effects of environmental conditions, there are also known helpful effects. These include weightlessness (in water) as a means of providing body movement exercise for injured persons, a warm environment to reduce the effects of body shock in accident situations, and pressurizing the body to allow body gases to dissolve while countering the effects of the bends. There have always been cases in which personnel have exceeded the usual survival limits—such as those in Fig. 10-1—and lived. Such "superhuman" efforts are not rare in the case of Army personnel who must survive under battle and other wartime conditions that impose extraordinary stresses.

Tolerance limits are extremes that most persons can endure without adverse effects. The safe exposure limits include a safety factor that will permit the most susceptible person to endure without adverse effect. For example, most persons can still live in an atmosphere in which the air contains only 16% oxygen. A safe exposure limit would be 18-19%, although OSHA regulations specify 19.5% for the work place. (That the oxygen level is less than the normal 21% may be a matter of concern; a decrease to 20% should be a reason for investigation of the cause even though the environment is still "safe".) Available limits for specific hazards will be noted in the discussions later in this chapter.

Table 10-5 (Ref. 15) lists the environmental factors that are considered "ideal". An examination of the data in Table 10-5 indicates that the ideal environments might exist in some areas of the world. With human assistance to limit the objectionable excesses and improve the others—such as adding light and work space—the ideal environment may be created in many other areas.

10-2.2 POTENTIAL HAZARD SOURCES

Potential hazards from natural and induced environments can usefully be divided into two categories. In the first category are those hazards that can be easily recognized as harmful to the human body. In the second category are environmental hazards that are insidious because their harmful effects are not so obvious. For example, in

TABLE 10-5. IDEAL ENVIRONMENT FOR MAN (Ref. 15)

1.	Temperature: 19°-21°C (68°-72°F)
2.	Relative humidity: 40-50%
3.	Ambient pressure: 101 kPa (14.7 lb/in².)
4.	Oxygen partial pressure: 18-21%
5.	Carbon dioxide partial pressure: 0.3-0.5%
6.	Daily water requirements: 2.3 kg (5 lb)
7.	Ozone and atmospheric pollution: 0
8.	Nuclear radiation: less than 40 milliroentgens per day
9.	Ambient illumination: 16 candela/meter² (5 millilamberts)
10.	Ambient random noise: 20 dB
11.	Allowable noise level: 55 dB(A)
12.	Air movement: 2.8 m³/min (100 ft³/min)
13.	Clothing: Shirt sleeves
14.	Minimum operational space: 18.4 m³/man (650 ft³/man)

the first category are the natural environments of cold and various forms of precipitation. Temperature (heat) can be in either category, depending on the degree and whether it is accompanied by high or low humidity. Various forms of radiation—solar, laser, X ray, and electromagnetic (radio or radar energy)—lie in the second category because the body does not necessarily perceive the immediate existence of a hazard. Consequently, for any Army program, all possible natural and induced environments must be considered as sources of hazards in the design of the system and the development of operational procedures.

10-2.3 ENVIRONMENTAL CONTROL TECHNIQUES

The first step in the control of an environmental hazard is to define it completely by means of the hazard analysis process. The designer then can evaluate the usefulness of various design features to eliminate or control the hazard. Considerations might weigh the suitability of enclosures of various types for both personnel and equipment or protective clothing for personnel only. In other examples, the designer might determine whether

1. Use of filters will prevent particulate matter such as dust and blowing sand from entering either the human respiratory system or equipment.

2. Various types of shields will prevent skin and eye burns from solar radiation. These shields could range

from rigid or flexible structures to skin creams and filtered glasses.

3. Induced environmental conditions in a particular design could be improved without degrading the performance of the equipment, e.g., radiating equipment of lower power where personnel are unavoidably exposed to the radiating pattern.

4. Environment can be improved by adding some external element such as adding heat to improve an environment that is too cold or removing heat from an environment that is too hot. The same approach can be used to control the hazards resulting from too much or too little moisture.

Additional techniques for the control of specific hazards existing in either the natural or induced environment are described under the specific hazard later in this chapter.

10-3 THERMAL HAZARDS

Thermal hazards—affecting personnel performance and causing equipment damage—may result from the uncontrolled flow of heat, high temperatures, low temperatures, or changes in temperature. These hazards may, by themselves, cause injury or damage, or they may contribute to the effects of other hazards.

Temperature is a man-made scale that indicates the level or perception of heat present in a body. Heat is a form of energy that will flow from the location of a higher temperature to one of a lower temperature. Thermal hazards occur when the flow of heat becomes uncontrolled and occurs in massive quantities. (See par. 9-2.)

Heat energy can be transferred by radiation, conduction, and convection, i.e.,

1. *Radiation*. The transfer of heat in the form of electromagnetic waves between two bodies, substances, or surfaces that are not in contact

2. *Conduction*. The transfer of heat by the motions of molecules from one portion to another portion of a substance without movement of the substance itself. In like manner, heat may be transferred by conduction from one substance to another when the two substances are in contact.

3. *Convection*. The transfer of heat through a liquid or gas by movement of the molecules within the fluid. Circulation of a fluid is a convection process caused by differences in the density of a fluid heated or cooled by whatever means—natural convection. The circulation can also be created by pumps, blowers, or agitators—forced convection.

Heat transfer may be a required process for particular systems to control maximum or minimum temperatures. Heat transfer, however, can also be an undesired process within a system design when a hot part—such as an exhaust manifold of an engine—transfers heat to a fuel pump and causes "vapor lock" and engine stoppage. In this instance, protective thermal shields should be added to the design to control the heat transfer. Alternatively, the fuel pump could be mounted in another location less affected by the high exhaust temperature. Likewise, the ignition coil must be located so as not to be subjected to a higher temperature than its materials can withstand.

The heat transfer process can create temperature extremes that are hazardous to people and/or equipment. High temperatures also increase the susceptibility of materials to fires and may cause their ignition. In addition, the heat available at high ambient temperatures can constitute part of the energy required to initiate a chemical reaction and thus lower the initiation level. Under these conditions the additional energy required to initiate the reaction may be quite small. An example is gasoline exposed to the atmosphere in extremely warm conditions. The elevated temperature causes rapid evaporation of the gasoline to produce an ignitable mixture with air present; then, little additional energy is required to ignite the mixture. Obviously, many sources can provide the ignition energy. For example, contact with a hot metal surface may be adequate to provide that energy. Consequently, gasoline spills that occur in open, sunlit areas are more dangerous than spills in shaded locations.

High temperatures may cause the charring or melting of organic solids and possibly their ignition. These high temperatures may be caused by chemical reaction (fire), friction, thermal radiation from hot surfaces, or direct contact with a hot surface. They also may be caused by friction, which is often an abnormality, and they may accompany a normal process such as the high temperatures associated with a steam boiler. High-temperature surfaces may be present in electronic equipment under normal or abnormal conditions.

Human tissue injuries (burns) are caused by thermal, electrical, or chemical agents. The extent of injury will depend upon the type of agent and its duration and intensity of action. Tissues in direct contact with the agent—e.g., the skin and sometimes the mucosa of the respiratory and gastrointestinal tracts—will be damaged most quickly, but the systemic effects of severe burns generally pose a greater threat to life than do local effects.

Thermal hazards cause direct injury to humans in two ways: tissue damage due to heat and interference with normal biological functions. Burns are categorized as first degree, second degree, or third degree, depending on the degree of tissue damage. Third-degree burns are the most severe.

For electrical burns, injury results from the generation of heat ranging up to 5000°C (9000°F). Since most of the resistance to electric current is at the point of skin contact with the conductor, electrical burns usually involve the skin and subjacent tissues and may be of almost any size and depth. Progressive necrosis (tissue death) and sloughing are usually greater than the original lesion (clearly circumscribed abnormality) would indicate. Electrical

burns are insidious in nature since the extent of injury to deep tissue is not readily apparent.

Chemical burns may be due to strong acids and alkalies, phenols, cresols, mustard gas, or phosphorus. All produce necrosis, which may extend slowly for several hours. Inhalation (respiratory tract) injury accompanying thermal burns is due to inhalation of the incomplete products of combustion, which are potent chemical irritants to the respiratory mucosa, or mucous membranes. Only steam inhalation results in actual thermal damage to the respiratory tract.

Most design criteria for military equipment have the same stipulations regarding hot surfaces as those in MIL-STD-1472 (Ref. 7) and MIL-STD-454 (Ref. 8), i.e., exposed parts will not have a temperature in excess of 60°C (140°F) at an ambient temperature of 25°C (77°F), and front panels and operating controls of electrical equipment will not exceed 49°C (120°F).

10-3.1 TOLERANCE AND SAFE EXPOSURE LIMITS

Radiant heat sufficient to cause first-degree burns may be generated by open flames or extremely hot surfaces. The higher the temperature or thermal transfer, the shorter the time required to cause damage. Fig. 10-4 (Ref. 16) indicates the thermal energy-time relationships necessary to cause pain from radiant heating; Fig. 10-5 (Ref. 16) indicates the relationship for convective heating. Table 10-6 (Ref. 16) covers the same relationships for conductive heating. The longer the exposure to a temperature high enough to cause a burn—see paragraphs that follow for threshold temperatures—the more severe will be the
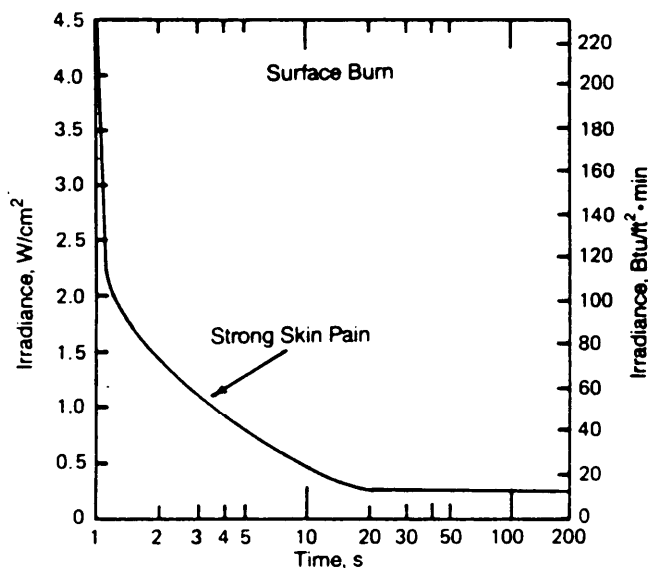
*To convert to W/m², multiply by 10⁴.

Figure 10-4. Pain From Radiant Heating (Ref. 16)
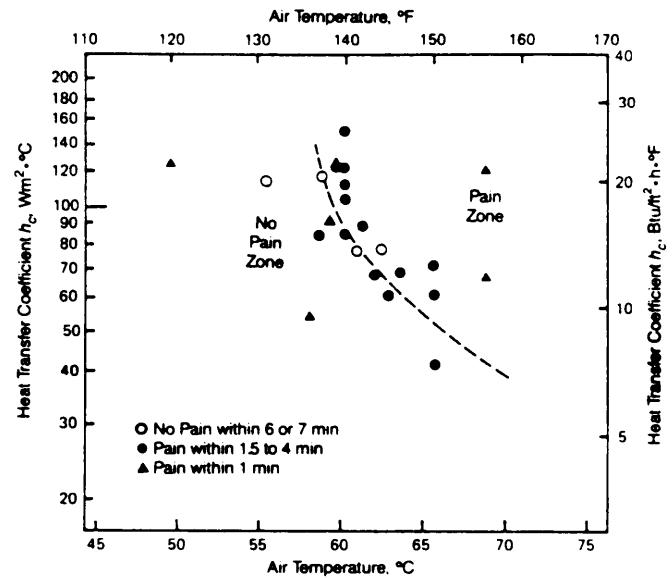
Figure 10-5. Pain From Convective Heating (Ref. 16)

category of burn (first, second, or third). The major effects of first-degree burns are discomfort and a resulting reduction in efficiency.

Fig. 10-4 shows the time intervals required for radiant heating to generate strong skin pain, using radiation sources ranging from the simulated intense thermal-flash of a nuclear weapon—approximately 315 W/m² (100 Btu/ft²·min)—to the slow heat-pulse associated with reentry heating, wherein the heating is partly convective. Note that for small skin areas the curve becomes asymptotic at about 57 W/m² (18 Btu/ft²·min), which means that at this level and below the blood supply to the skin is carrying off the heat as fast as it arrives, and heat is stored in the body. How long this process can be sustained with total body exposure has not been established.

The data in Fig. 10-5 indicate the dividing line between painful and nonpainful effects from heating by air at various temperatures versus the heat transfer coefficient h_c, which depends on air density, air velocity, and surface area and shape. The data were obtained by exposing a small segment of the cheek to an air stream flowing through a padded hole in the wall of a cylindrical tube. h_c was computed from air velocity and duct geometry.

Simple precautions will prevent most cases of severe sunburn. Initial summer exposure to bright, midday sun should not exceed 30 min, even for persons with dark brunette skin. In temperate zones sunburn-producing wavelengths are usually filtered out before 1000 h (10 A.M.) and after 1600 h (4 P.M.), and exposure is less hazardous at those times. Commercially available sunscreen lotions are very effective in preventing sunburn.

Each system under development should be analyzed to reveal all possible sources of high temperatures that could result from equipment operation or from malfunction. If

TABLE 10-6. PAIN FROM CONDUCTIVE HEATING (Ref. 16)

Body Area	Clothing Worn	Metal Surface Temperature °C	°F	Average Tolerance Time, s
Hand	Bare skin	48	120	10-15
Kneecap	Bare skin	47	117	34
	Bare skin	48	120	5
Fingertip	AF/B-3A leather gloves	65	150	12.6
	AF/B-3A leather gloves	71	160	7.3
Palm of hand	AF/B-3A leather gloves	65	150	25.2
	AF/B-3A leather gloves	79	175	9.7
	AF/B-3A leather gloves	85	185	8.0
Forearm	SAC alert suit	65	150	20.6
	SAC alert suit	79	175	8.0
Upper arm	K-2B light AF flight coverall	65	150	7.5
	SAC alert suit	65	150	31.3
	Alert suit plus Brynje net string underwear	149	300	7.2
	K-2B suit	65	150	18.1
	K-2B suit plus Brynje underwear	65	150	61.9
Buttocks	SAC alert suit	65	150	70.3
	Alert suit plus Brynje underwear	149	300	21.7
	K-2B suit	65	150	32.5
	K-2B suit plus Brynje underwear	65	150	+90
Mid-thigh	SAC alert suit	65	150	35.6
	Alert suit plus Brynje underwear	149	300	13.1
	K2-B suit	65	150	13.6
	K-2B suit plus Brynje underwear	65	150	+90
Kneecap flexed	SAC alert suit	65	150	14.4
	Alert suit plus Brynje underwear	79	175	9.5
	K-2B suit	65	150	7.3
Calf muscle	SAC alert suit	65	150	14.4
	Alert suit plus Brynje underwear	149	300	11.4
	K-2B suit	65	150	13.2
	K-2B suit plus Brynje underwear	65	150	66.1
Upper arm	MD-3A wool-nylon antiexposure suit	149	300	12.0
	MD-3A wool-nylon antiexposure suit	204	400	10.2
Forearm	MD-3A suit	121	250	15.9
Palm of hand	Aluminized asbestos glove	121	250	13.5
Back of hand	Aluminized asbestos glove	121	250	5.2
Palm of hand	Arctic mitten	149	300	18.7
	Arctic mitten plus B-3A glove	149	300	37.0
	Arctic mitten plus B-3A glove	204	400	27.6
	Pigskin 427°C (800°F) heat glove	149	300	30.7
	Pigskin 427°C (800°F) heat glove	204	400	21.0
	Pigskin 427°C (800°F) heat glove	260	500	18.5

Notes: Light touch pressure (less than 1 psi)—6.9 kPa—applied to heat metal surface. The elbow and knee sometimes receive second-degree burns without pain.

a hazard is present, the designer must attempt to provide protection by eliminating the sources of high temperature. When elimination is not possible, barriers must be provided to isolate personnel from known high-temperature sources and from materials or surfaces that have high temperatures.

Another manner in which high temperature affects man directly is by upsetting his biological balance. Table 10-7 (Ref. 15) indicates normal tolerable limits of temperature. The body rids itself of excess heat primarily through evaporation of perspiration. To a lesser degree, radiation, conduction, and convection also serve to transfer heat from the body. If high-temperature environments overload these cooling processes, the metabolic processes may be upset; this can cause heat cramps, heat exhaustion, or heat stroke. Table 10-8 (Ref. 16) provides some correlating data among debilitating heat disorders, their causes, symptoms, and prevention and first aid.

Even when elevated temperatures do not result in illness or injury, they will degrade performance. Figs. 10-6 (Ref. 8) and 10-7 (Ref. 17) and Table 10-9 (Ref. 15) contain data relating elevated temperatures with degradation of the human ability to perform certain functional processes. The effects of high levels of heat and humidity on physical activity were investigated in a series of tests. In each test, Fig. 10-6(B), 16 Army enlisted men marched at 4.8 km/h (3 mph) for 4 h with a 9-kg (20-lb) pack in a controlled room. Observation of these men made it possible to characterize their performance as relatively easy, difficult, or impossible. The results emphasize the importance of humidity in combination with temperature as a factor limiting the performance of such tasks. For any

given temperature, such as 37.8° C (100° F), the difference between ability to do the job versus not being able to do it is a matter of a small percentage of change in relative humidity. The threshold point for human performance degradation depends on the combined effects of temperature, time, humidity, exertion, physical and mental condition, acclimatization, and stress from other sources.

Human engineering criteria and guidelines provide information on human tolerance to heat and temperature. Where sources of heat and temperature cannot be eliminated, the operators or occupants should be provided with life support systems. In developing such equipment, the designer must consider the sources of heat and both the natural and induced environments to be encountered.

Increases in temperature will affect chemical reactions, the behavior of fuel/air mixtures, the pressure of gases and liquids, and the reliability of electronic equipment. High temperature will cause fuels to explode rather than to burn normally, accelerate corrosion, create instability in chemical processes, and cause increased failures due to rupture of gas and liquid containers. When temperatures reach very high levels, metals will lose their strength and eventually become molten.

Sensitive avionics and other electronic instruments in Army aviation vehicles and other mobile equipment must be protected from temperatures above the design limits. Increased failure rates will result from unprotected operation or storage at over-the-limit temperatures. When special operations are to be performed at temperatures above the normal design specification for the equipment, there are two alternative design approaches. First, the equip-

TABLE 10-7. TOLERABLE LIMITS OF TEMPERATURE (Ref. 15)

Condition	Temperature, °C (°F)
Comfort zone, summer	13.3°-23.9°(56°-75°)
Comfort zone, winter, light work	17.2°-21.7°(63°-71°)
Comfort zone, winter, heavy work	12.8°-15.6°(55°-60°)
Physiological limits, at rest, heat	68.9°(156°) for 30 min at 10% humidity 41.7°(107°) for 30 min at 90% humidity 260°(500°) for 2 min air dry 93.3°(200°) for 35 min air dry 50°(122°) for 120 min air dry
Physiological limits, at rest, cold	3.3°(38°) for 5 h at 4.8 km/h (3 mph) air velocity 6.7°(44°) for 4 h at 14.5 km/h (9 mph) air velocity
Physical stiffness of extremities begins	10°(50°) and under
Physical fatigue begins	23.9°(75°) and over
Mental activities and complex performance begin to deteriorate	29.4°(85°) and over

TABLE 10-8. CLASSIFICATION OF DEBILITATING EFFECTS OF HEAT (Ref. 16)

Disorder	Cause	Symptoms	Preventive and First Aid
Heat Cramps	Excessive loss of salt in sweating with inadequate replacement.	Pain and muscle spasm; pupillary constriction with each spasm. Body temperature normal or below normal.	Normal diet and fluid intake. Rest, administer salt and water.
Heat Exhaustion	Cardiovascular inadequacy; dehydration.	Giddiness; headache; fainting; rapid and weak pulse; vomiting; cold, pale, clammy skin; small rise in body temperature.	Frequent and early replacement of water, frequent pauses. Rest in shade in recumbent position. Administer fluids.
Heat Stroke	Failure of temperature regulatory center, due to excessively high body temperature.	High body temperature; irritability, prostration, delirium; hot, dry, flushed skin. Sweating diminished or absent.	Adequate pacing of activity, avoidance of severe effort by unacclimatized people in hot environment. Alcohol spray bath or immersion in cold water. Medical emergency requiring a physician.

ment can be provided with additional thermal protection such as thermal reflector panels or radiator units to cool the equipment. Second, similar equipment, thermally upgraded by design, can be substituted for the less thermally resistant equipment. As always, the design solution can be found by a thorough analysis of all factors that will affect the required operating performance of the equipment.

The opposite extreme of heat can be equally hazardous. Low temperatures can cause freezing with tissue damage and degradation in human performance. Wind will increase the loss of heat and, consequently, enhance the effects of low temperature. Fig. 10-8 (Ref. 15) relates wind and temperature and their effects on humans. In cold weather outdoors, the wind velocity has a profound, sometimes decisive, effect on the hazard to personnel who are exposed. The windchill concept dramatizes this well-known fact by providing quantitative comparison of various combinations of temperature and wind speed. Note from Fig. 10-8, for example, that −40°C (−40°F) with air movement of 0.1 m/s (0.3 ft/s) (See Line B.) has the same windchill value—and, therefore, the same sensation on exposed skin—as −24°C (−13°F) with a 0.5-m/s (1.5-ft/s) wind. (See Line A.)

The windchill index does not account for physiological adaptations or adjustments and should not be used in a rigorous manner. The index is based on field measurements by Paul Siple during World War II of the rate of cooling of a container of water. The values of windchill factor K_o in Fig. 10-8 have been calculated using the equation

$$K_o = (\sqrt{WS \times 100} - WS + 10.5)$$
$$(33 - T_a), \text{kcal/m}^2 \cdot \text{h} \qquad (10\text{-}1)$$
$$= 4.184(\sqrt{WS \times 100} - WS + 10.5)(33 - T_a), \text{MJ/m}^2 \cdot \text{h}$$

where
WS = existing wind speed, m/s
T_a = existing dry-bulb temperature, °C.

Note: On the wind speed scale, the 0.01-mile-per-hour point is displaced from the meter-per-second scale because the two scales are logarithmic.

Low temperatures also reduce the absolute humidity; in winter outside cold air becomes so dry that it is conducive to the generation of static electricity. When this same dry air is warmed indoors by a heat source, the relative humidity decreases farther.

Conditions	Energy Expenditure Rate, W(Btu/h)	Air Temperature Necessary—Assuming Appropriate Clothing—for Thermal Balance at Air Movement Rates of		
		6.1 m/min (20 ft/min)	3.5 m/min (100 ft/min)	32.2 km/h (20 mph)
At Rest	117 (400)	21.1°C (70°F)	22.8°C (73°F)	25.6°C (78°F)
Moderate Activity	293 (1000)	14.4°C (58°F)	15.6°C (60°F)	17.2°C (63°F)
Vigorous Activity	1172 (4000)	−2.2°C (28°F)	−1.1°C (30°F)	1.7°C (35°F)

(A) Necessary Air Temperature
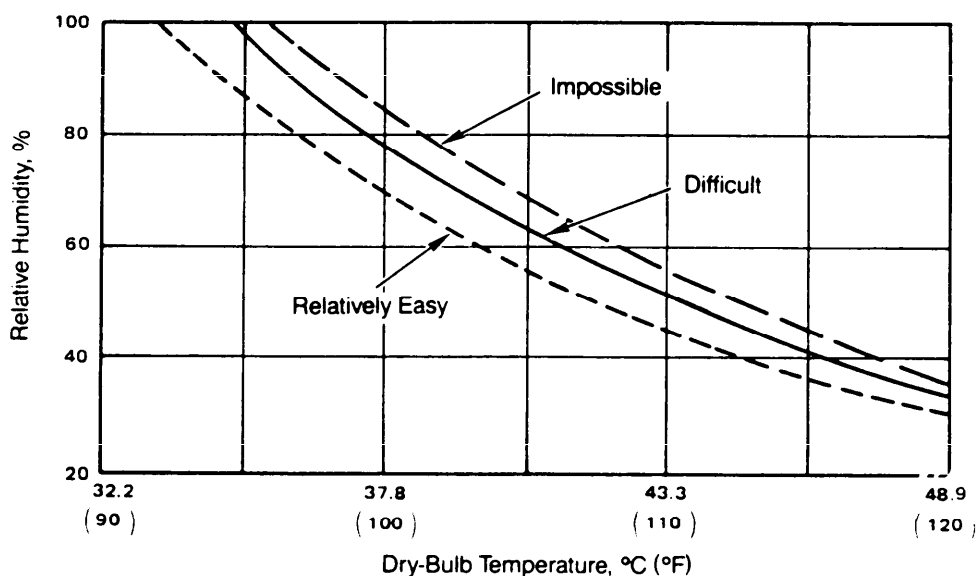
(B) Effect of Humidity on Human Performance

Figure 10-6. Relative Difficulty of Performing a Marching Task Under Various Temperature and Humidity Conditions (Ref. 8)

When humans protect themselves with heavy clothing to perform work in very cold weather, the bulk of the clothes further degrades performance. Designers must consider that heating systems may fail in cold climates, and human operators will have to resort to protective clothing. This will affect the design of controls and switches; making a crew station too comfortable, however, will decrease attentiveness. In accordance with MIL-STD-1472 (Ref. 7), human engineering provides design guidance for cold-related problems and should be used in designing against cold as well as against heat.

Cold temperatures also adversely affect machines. At low temperatures, metals, plastics, and rubber become brittle or stiff and susceptible to failure. Liquids freeze or become highly viscous and resist flow or burst their containers. Fuel will not vaporize readily, and ignition becomes difficult.

10-3.2 POTENTIAL HAZARD SOURCES

Sources of heat that can affect Army systems are present in the natural environment and can also be generated by equipment and personnel. Enormous inputs of heat from solar energy can be experienced in tropical, desert, and mountainous areas. The effects of these inputs are multiplied in enclosed spaces with no natural or mechanical cooling since the contained persons are generating additional heat. Not only do the metabolic processes of persons in restricted spaces elevate temperatures, but they also increase the humidity until the combination of temperature and humidity becomes intolerable. Such conditions can occur not only in tanks and closed personnel carriers but also in impermeable suits required for NBC warfare.

In the natural environment low temperatures occur in arctic climates, mountains, deserts, and other open land masses that reflect much heat into space during winter. In induced environments, refrigerated equipment can generate moderately low temperatures; equipment with cryogenic cooling can generate very low temperatures. Windchill can become a factor anyplace there is movement of cold air, and it need not be in the open environment.
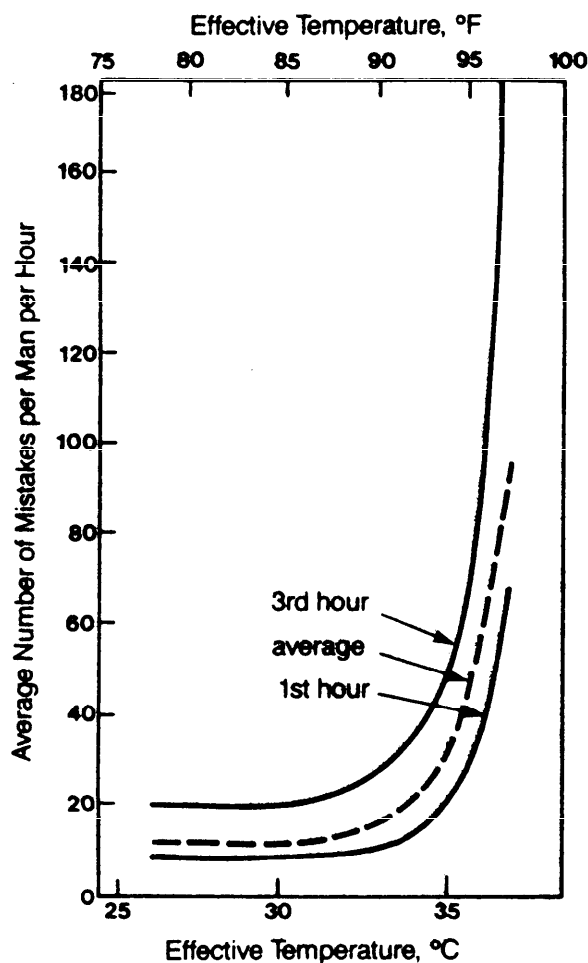
Figure 10-7. Error Increase Due to Rise in Effective Temperature (Ref. 17)

10-3.3 HAZARD CONTROL TECHNIQUES

The best means of controlling thermal hazards is to keep temperatures within moderate ranges and to control heat flow. Cooling systems can be used when excessive heat is the result of the natural environment, generated by the equipment, or both. Fig. 10-9 (Ref. 15) indicates how the flow of radiant heat from a high-temperature source can be controlled with heat shields. The conductive flow of heat can be reduced by cooling the conductor, by interposing a nonconductive material in the flow path, or by using heat sinks. The convective flow of heat can be reduced by placing a thermal barrier between the area of convective flow and the subject or object—e.g., insulated clothing, covers, or shields. MIL-STD-1472 (Ref. 7) provides criteria for controlling the thermal element of the environment as follows (see Fig. 10-10 (Ref. 7) for the relationship between dry-bulb (DB) temperature and effective temperature (ET)):

1. *Heating*:

    a. Within Mobile Personnel Enclosures: above 10° C (50° F) DB
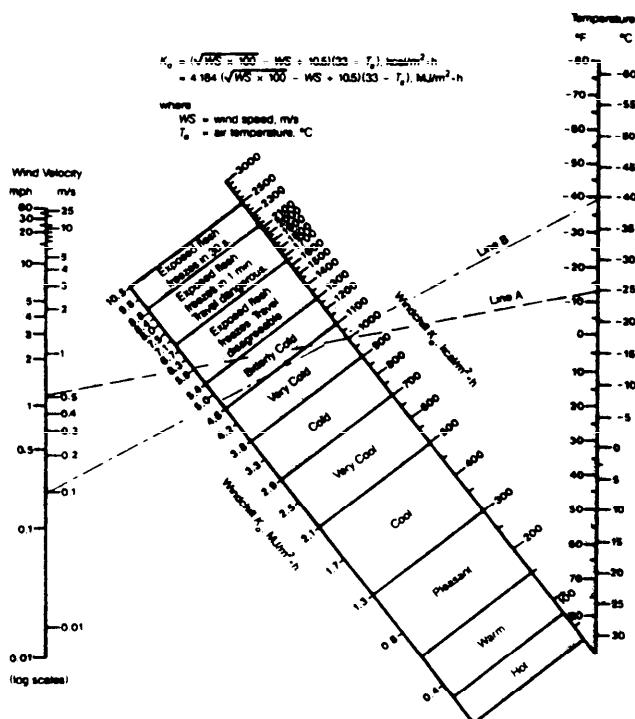
Figure 10-8. Windchill (Ref. 15)
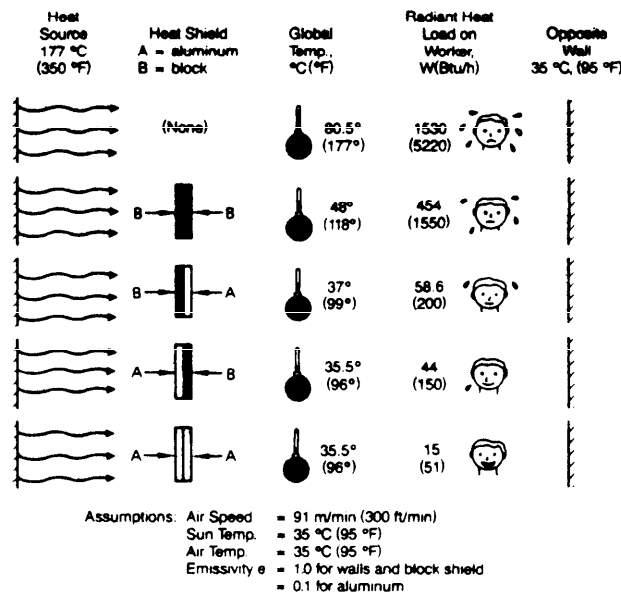
Figure 10-9. Use of Shields as Means of Reducing Radiant Heat Load From Hot Surfaces (Ref. 15)

TABLE 10-9. CRITICAL EFFECTIVE TEMPERATURES AT WHICH IMPAIRMENT MAY BE DEMONSTRATED, ACCORDING TO VARIOUS SOURCES (Ref. 15)

Name and Type of Test	Investigator	Temperature			
		Max. at Which Performance Remains Normal,		Demonstrable Impairment,	
		°C	°F	°C	°F
Typing scrambled letters	Viteles	26.7	80	30.6	87
Morse code reception	Mackworth	30.8	87.5	33.3	92[a]
Locations (spatial relations code)	Viteles	26.7	80	30.6	87
Block coding (problem solving)	Mackworth	28.3	83	30.8	87.5[a]
Mental multiplication (problems)	Viteles	26.7	80	30.6	87
Number checking (error detection)	Viteles	26.7	80	30.6	87[a]
Visual attention (clock test)	Mackworth	26.1	79	30.8	87.5[a]
Pursuit (visual maze)	Viteles	26.7	80	30.6	87
Reaction time (simple response)	Forlano	33.9	93[b,c]	—	—
Discrimeter (complex response)	Viteles	26.7	80	30.6	87
Lathe (hand coordination)	Viteles	26.7	80	30.6	87[a]
Pursuitmeter	Mackworth	30.8	87.5	33.3	92[a]
Motor coordination	Weiner	18.1	64.5[c]	32.8	91[a]
Ergograph (weight pulling)	Mackworth	27.2	81[d]	29.6	85.3[a,d]
Bicycle ergometer (heavy work)	Liberson	18.1	64.5[c]	33.1	91.5[c]
Weight lifting (heavy work)	N.Y. Ventilation Committee	18.1	64.5[c]	21.1	70[c]

[a]Deterioration statistically significant
[b]Provided wet bulb does not exceed 30°C (86°F)
[c]Effective temperature estimated from data in report
[d]Midpoint of a range of conditions

b. Within Permanent and Semipermanent Facilities: 18°C (65°F) ET or above unless directed otherwise by workload or extremely heavy clothing

c. Discharge: directed away from personnel

2. *Ventilation*:

a. Volume Ratio: minimum of 0.85 m³/min·person (30 ft³/min·person); approximately two-thirds of the volume should be fresh, outside air

b. Speed: 30 m/min (100 ft/min) or less; 20 m/min (65 ft/min) preferred

c. Intake Locations: Located to minimize the introduction of contaminated air, e.g., from exhaust pipes

d. Contaminants: Limits on gases, vapors, dust, and fumes will be within those specified by the threshold limit values set by the American Conference of Governmental Industrial Hygienists.

3. *Air-Conditioning*:

a. Within Enclosures: at or below 29.4°C (85°F) ET

b. Discharge: directed away from personnel

4. *Humidity*. Approximately 45% relative humidity at 21°C (70°F) DB. This value should decrease with rising temperature but should remain above 15% to prevent irritation and drying of body tissues—e.g., eyes, skin, and respiratory tract.

5. *Temperature Uniformity*. Temperature of air at floor level and at head level should not differ by more than 5.6 deg C (10 deg F).

6. *Personal Equipment Thermal Control*. Microclimate between 20°C (68°F), 1.9 kPa (14 mm Hg) ambient water vapor pressure and 35°C (95°F), 400 Pa (3 mm Hg) is desirable and where possible should be maintained by the heat transfer system when special protective clothing or personal equipment—including full and partial pressure suits, fuel handler suits, body armor, arctic clothing, and temperature-regulated clothing—are required and worn.

7. *Thermal Tolerance and Comfort Zones*. Temperature and humidity exposure should not exceed the effective temperature limits indicated in Fig. 10-11 (Ref. 13) when corrected for air velocity in Fig. 10-10 (Ref. 7).

8. *Limited Thermal Tolerance Zones*. Where hard physical work is required for more than 2 h, an environment not exceeding a WBGT index—see paragraph that follows for discussion of WBGT—of 25°C (77°F) shall be provided. Where the wearing of protective clothing systems that reduce evaporation of perspiration from the

Note: To use nomograph, draw straight line between dry-bulb (DB) temperature A and wet-bulb (WB) temperature B. Effective temperature (ET) is indicated where this straight line crosses the appropriate value for velocity of air. (In this example, ET is 21 °C (69 °F) for DB of 24 °C (76 °F), WB of 17 °C (62 °F), and air velocity of 30 m/s (100 ft/min).

Clothing: Customary indoor clothing

Activity: Sedentary or light muscular work

Heating Methods: Convection type—i.e., warm air, direct steam or hot water radiators, plenum systems

Figure 10-10. Deriving Effective Temperature (Ref. 7)

skin is required, the index shall be decreased 5 deg C (10 deg F) for complete protective uniforms, 4 deg C (7 deg F) for intermediate clothing systems, and 3 deg C (5 deg F) for body armor.

For military personnel who must work outside in hot climates—in ranges beyond the comfort and discomfort zones of heat stress—the Wet-Bulb Global Temperature (WBGT) Index is more applicable than the ET Index. The WBGT Index takes into consideration dry-bulb temperature; relative humidity calculated with ambient air movement, rather than at a standardized rate; and the solar, or radiant, heat load. This index and its use are described in Ref. 18. The WBGT is calculated as follows (Ref. 13):

$$WBGT = 0.7T_{WB_{np}} + 0.2T_g + 0.1T_A, \ °C(10\text{-}2)$$

where

$T_{WB_{np}}$ = natural, wet-bulb, nonpsychrometric temperature, °C (Temperature read from a "natural" wet-bulb thermometer with a wettable wick exposed to ambient air motion and extending into a water reservoir.)

T_g = temperature, representing radiant heat, measured at the interior of a 152-mm (6-in.) black globe, °C

T_A = shaded dry-bulb air temperature, °C.

Generally, the activities of unacclimatized individuals are restricted when the WBGT exceeds 25° C (77° F) (Ref. 13).
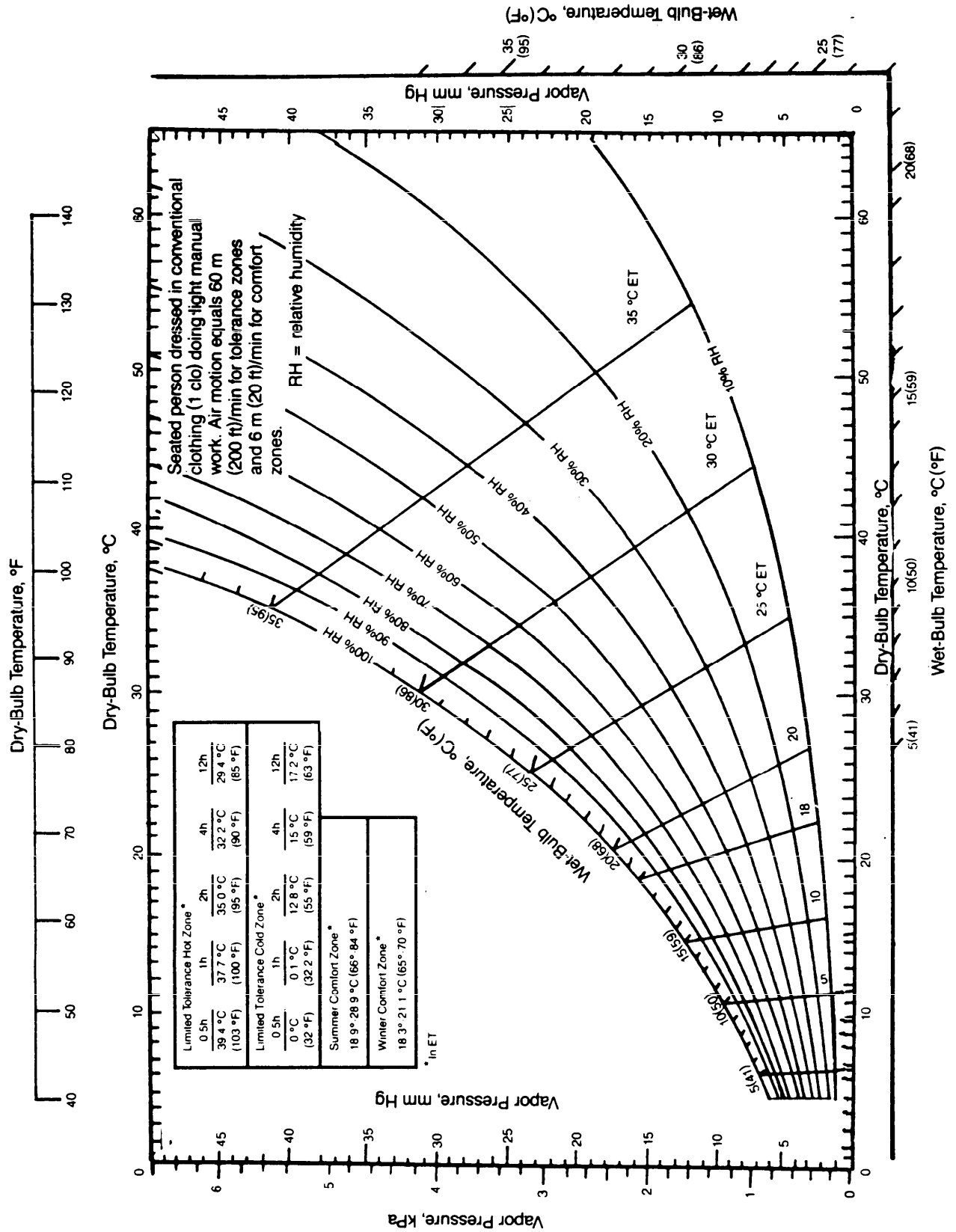
Figure 10-11.   Summer and Winter Comfort Zones and Thermal Tolerance for Inhabited Compartments (Ref. 13)

10-3.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

Guidelines for the solution of thermal problems follow:

1. As early as possible in the acquisition process, complete a thermal analysis for each proposed component of a design to determine its hot and cold characteristic conditions.

2. As the design progresses, conduct thermal analyses of multiple components of the subsystems and the system. During this continuing analysis, determine the thermal interactions and redesign for more favorable thermal conditions when either personnel or equipment will be unacceptably affected by the thermal characteristics of the design. When redesign is not possible due to performance, manufacturing, schedule, or cost limitations, use the following criteria to protect personnel and equipment:

　　a. Provide in-place insulation and/or thermal radiant shields between the equipment and personnel.

　　b. When the action in par. 2a is not sufficient, provide protective clothing with insulation and radiant shields.

　　c. Specify that the structure and parts that must come in contact with personnel be made from materials with low or high thermal conductivity in accordance with the requirement to prevent or facilitate heat flow.

　　d. When there is no other practical solution to controlling higher temperature environments, provide cooling subsystems such as mechanical refrigeration units.

　　e. When there is no other practical solution to controlling low-temperature environments, provide heating subsystems.

　　f. When equipment must be capable of safe performance while undergoing relatively large temperature variations, design expansion joints into the equipment and/or specify that mated surfaces of parts be fabricated from materials with similar coefficients of thermal expansion. Consider the effects of these measures upon the total system.

　　g. Specify materials with thermal strength capabilities well above the expected thermal environment for the part being designed. Use a larger thermal safety factor if the thermal environment cannot be predicted with accuracy. (Increase the temperature specification as much as 25 to 50% above the estimated maximum operating temperature if the estimate of the thermal environment cannot be related to similar field-tested equipment or conditions.)

　　h. Specify lubrication subsystems and lubricants that have been field tested and approved by the Army to withstand the thermal environment.

　　i. When thermally sensitive hazardous materials are present in the system, insure that the routings of heat-producing elements are separated from the locations of the hazardous materials to the maximum extent possible in the design.

　　j. When the performance of the equipment would be affected by thermal changes, e.g., optical sighting devices, design thermal compensation devices into the unit.

10-4 PRESSURE

Either positive or negative pressures can constitute a hazard. Pressures need not be great to cause catastrophic damage if the medium containing them fails.

Winds with pressures of less than 6.895 kPa (1 psi) have generated tremendous damage, both by the forces they exert over large surfaces and by the solid matter they can carry. If this pressure of 6.895 kPa (1 psi) is imposed on a surface of 1.016 m × 1.016 m (40 in. × 40 in.), the total force on the surface is 7.117 kN (1600 lb). If this surface is a glass observation window and only a 0.508-m × 0.508-m (20-in. × 20-in.) section in the center of the viewing window is considered, this center section must withstand 1.779 kN (400 lb). If the wind suddenly ceases, the force drops to zero or becomes negative (opposite to the initial force), and opposite stress can cause sufficient movement to break the glass. Similar considerations must be part of the safety analysis for any equipment that can be subjected to changing pressures. In addition, whenever a pressure system must be specified, the pressure should be kept to the minimum required for the task.

Negative pressures in closed containers are created in a number of ways that must be considered in the design of containers. For example, a low-pressure container closed and sealed in a high-altitude location, such as Denver, CO, could be crushed if it is moved to a sea level location because of the relatively high outside pressure. This same phenomenon can occur in the radiator and hoses of an Army vehicle when the engine has been turned off and it cools down. One method of preventing damage to a closed container under changing pressures is to open the container so that it can freely receive or discharge a gaseous substance. The containers can be opened by means of a relief valve to permit the passage of air or some gas (air substitute such as dry nitrogen) or liquid into or out of the container to avoid a destructive positive or negative pressure.

Negative pressures are also encountered during the negative phase of passage of a blast wave or a weather phenomenon such as a tornado. Equipment that can survive these conditions must either be sufficiently rugged to maintain its mechanical integrity under the expected conditions or be sufficiently flexible to deform in two opposite directions—under the positive and then negative pressure—without permanent damage.

One of the most common pressure hazards is the rupture of a pressure vessel. The effects will depend on whether the pressure medium is a gas or a liquid. Hydrau-

lic pressure systems are generally considered safer from a pressure standpoint than pneumatic ones, which may create shock waves in the surrounding atmosphere. Since liquid is considered incompressible, the work done in raising the liquid to a higher-than-ambient pressure is very little, almost insignificant, compared to the work required to raise a gas to the same elevated pressure. This difference in work represents a difference in stored, or potential, energy. Therefore, a gas subsystem under high pressure has a relatively high potential for creating a hazard in the event of a rupture. When a gas under pressure is released from a ruptured container, it continues to expand and to propel fragments. A gas jet escaping from an unsecured container will propel the container exactly like a rocket engine. The acceleration and velocity that result are a function of the container weight, gas pressure and volume, and the flow area of the opening through which the jet escapes.

Such is not the case with liquids because, as soon as a liquid under pressure is released, it expands only to its volume for that temperature. Liquids under pressure due to a hydrostatic head, however, continue to stream from a ruptured vessel with damaging force until the hydrostatic pressure has been relieved. In cases of massive rupture of a large liquid vessel, the released mass of liquid contains tremendous potential energy that immediately becomes kinetic.

Both liquid and gas pressure systems are subject to the effects of increased temperature, which causes expansion and increases the fluid volume or increases the pressure if expansion is restricted. Therefore, in designing a system that contains pressure subsystems, it is important to consider the effects of the pressure medium and ambient temperatures.

When a pressure system ruptures, its fittings, plugs, and gages may become dangerous projectiles that can cause severe injury. Jets of escaping pressurized gas are especially hazardous because thin, high-pressure jets of gas can cut the skin and carry debris that can cause injury or damage by impact. Gas jets have the potential to be more dangerous than liquids because gases cannot usually be seen.

Breaks in pressurized lines will cause an unsecured end to whip with a force proportionate to the pressure of the escaping liquid or gas. Even an unsecured, low-pressure garden hose can whip with sufficient force to cause injury if it strikes the face or other delicate body area. Accordingly, pressure lines should be as short as possible, secured at short intervals, and never flexible unless absolutely necessary.

Leaks in pressure systems can create additional hazards. For example, a leaking flammable gas or liquid will constitute a fire hazard. Escaping liquids are particularly hazardous because the sprays that generally occur are more easily ignitable than pools of liquid. Leaking flammable fluids may enter openings and passages in equipment and thus make the source of the leak difficult to trace; the fluid may travel great distances to reach an unexpected source of ignition.

Many flammable gases, and vapors from liquids, are heavier than air and will flow down a grade and collect at low points. The distance to the ignition source will determine how far the material will spread before ignition occurs. If the original spill or leak was a finite amount, the resulting fire will be limited in size and duration. If the leak continues, the resulting fire will not be limited and will depend on the rate of leakage.

Leaks of toxic gas and liquid can cause hazards to personnel for great distances beyond the source of the leak. Also a very small amount of toxic gas or liquid released into an enclosed area can be lethal. For example, carbon monoxide from a leaky exhaust system into occupied spaces of tanks, personnel carriers, or other vehicles can be fatal.

Leaking liquids may cause lubricity hazards by making surfaces slippery. Consequently, mobile equipment may slide or be unable to obtain the friction necessary to move, or persons may slip and fall. A leaking fluid may contaminate materials, supplies, or equipment. Corrosive gases or liquids may damage and weaken metals.

Loss of pressure because of leaks may cause items such as air brakes, hydraulic transmissions, or pneumatic power units to become inoperative. Cooling systems that have lost refrigerant or coolant will fail to cool units as intended, and these units may then overheat and malfunction. Loss of lubricants through leaks will also cause downstream units to overheat and fail; if rotating parts seize, they can cause large-scale damage to the equipment.

Any liquid pressure system in which the fluid moves will be subjected to the phenomenon of hydraulic shock, or "hammer". A moving liquid possesses momentum equal to the product of its mass and velocity. If this mass is suddenly stopped, a shock wave will develop in the liquid because it is very nearly incompressible. This shock wave will be transmitted throughout the liquid, including back upstream, and can exert tremendous force against the lines and vessels in which the liquid is contained. Connections, valves, and fittings can rupture.

If liquid is somehow introduced into a gas line, such as by condensation, it may be carried as a "slug" ahead of the gas. This often occurs when a steam system is shut down and then restarted. If no provision has been made to drain the lines and the system is restarted, the incoming steam will carry the liquid up front until it hits an obstacle, such as a fitting, and possibly fractures it.

10-4.1 TOLERANCE AND SAFE EXPOSURE LIMITS

Almost all natural conditions in which pressures differ substantially from the standard sea level atmosphere are dangerous to personnel. Many of these abnormal circumstances are commonly encountered by the other services, but few such abnormalities affect Army systems. Army aircraft generally do not operate at the high altitudes where air becomes so rarefied that it presents a danger. However, many Army aircraft are capable of flying at these altitudes and may at times be required to do so. Army personnel commonly do not work in compressed-air environments in which the bends would constitute a hazard; however, situations could arise in which exposure to such environments would be required. Also troops might have to operate at very high mountain elevations. Therefore, information on tolerances and safe exposure limits for these environments is included.

Pressure is commonly measured in millimeters of mercury (mm Hg) or pounds per square inch (psi) in the English system of units and in pascals (Pa) in the metric system. In diving, pressure is often expressed in units of depth, i.e., meters or feet of sea water, or atmospheres (atm). One atm is the average barometric pressure at sea level—101.3 kPa (760 mm Hg or 14.7 psi). With underwater descent, the ambient pressure increases rapidly. Every 10.06 m (33 ft) of descent in sea water adds 1 atm to the pressure encountered at that depth. The total (absolute) pressure exerted upon a submerged object is the pressure of the water plus the atmospheric pressure. Therefore, at 10.06 m (33 ft) below the surface, the total pressure is 2 atmospheres absolute (atm abs or ata); at 20.1 m (66 ft), 3 atm abs; etc. As external pressure increases with increasing depths, the gas pressure in the lungs, airways, and other tissues increases correspondingly; the gas pressure decreases when surfacing. The increase and subsequent decrease in pressure can produce significant physiological effects on the body, e.g.,

1. Vertigo due to disturbances in the inner ear
2. Accentuated overexertion resulting in respiratory exhaustion and general fatigue for scuba divers due to breathing denser air
3. Overinflation of lungs due to expansion of pulmonary gas on ascent
4. Gas embolism (air bubbles in blood vessels) and bends (decompression sickness) due to a rapid reduction in air pressure on ascent. Table 10-10 presents information on these two important physiological effects. Accordingly, adequate training is absolutely essential for safety in diving. Courses sanctioned by national organizations are widely available (Ref. 19).

For mechanical pressure systems in Army equipment, no exposure to pressures above 500 Pa (0.07 psi) gage should be considered safe. Thus all activities that require work on a pressurized system should require the use of protective personal equipment if the system cannot be shut down.

The Occupational Safety and Health Administration (OSHA) limits the pressure of air systems for cleaning to 207 kPa (30 psi) when closed end jets, i.e., no side opening for air to escape when the end is blocked, are used. The limit value of 207 kPa (30 psi) is recommended even when safety jets are used. Protective equipment such as transparent plastic fan shields is necessary because blown particulate matter may hit the person using the air system. Injuries have resulted from these relatively low-pressure subsystems during undisciplined conduct when the jet was directed at some person's body orifice.

10-4.2 POTENTIAL HAZARD SOURCES

Pressure hazards exist whenever a gas is contained and its pressure is increased above the ambient atmospheric pressure or whenever a liquid is contained and a force is applied to it.

Direct sources of pressure hazards are
1. A liquid or gas under pressure
2. A closed liquid or gas subsystem subject to increases in temperature
3. A closed liquid subsystem subject to hydrostatic pressure
4. Open liquid systems subject to hydrostatic pressure
5. Cryogenic liquid in a closed container that may be subjected to any heat input.

Indirect sources of pressure hazards are
1. Leakage of a flammable, corrosive, toxic, radioactive, or slippery fluid
2. Exhaustion of a cooling gas or liquid
3. Exhaustion of a lubricant so that other mechanical systems fail
4. Exhaustion of the liquid or gas that acts as a power transmitting medium so that units such as hydraulic brakes fail to operate
5. Propulsion of debris and contaminants carried by an escaping gas or liquid
6. Displacement of atmospheric oxygen by leakage of an inert gas
7. Impacts by high-velocity fragments from ruptured vessels
8. Impacts by whipping hoses
9. Impacts by cylinders or other containers propelled by gas or liquid escaping at high velocity.

10-4.3 HAZARD CONTROL TECHNIQUES

One of the most effective means of avoiding problems with pressure subsystems is to use the lowest possible pressure that will still permit the system to accomplish its intended mission. This will tend to minimize stresses on the components that can rupture or leak and will avoid or minimize many of the other hazards of high-pressure

TABLE 10-10. CONDITIONS REQUIRING RECOMPRESSION (Ref. 19)

	Decompression Sickness	Gas Embolism
Signs and Symptoms	Extremely variable. Three main types (singly or in combination): 1. "Bends"—pain, most often in or near a joint 2. Neurologic involvement of almost any type or degree 3. "Chokes"—respiratory distress followed by circulatory collapse (extreme emergency)	Common. Unconsciousness, often with convulsion Less common. Milder cerebral manifestations (Mediastinal and subcutaneous emphysema and/or pneumothorax may also be present.) Assume that any unconscious diver has gas embolism and seek recompression promptly.
Onset and Immediate Course	Gradual or sudden onset during decompression or as long as 24 h after dive* deeper than 9.1 m (30 ft) (or hyperbaric exposures beyond 2 atm abs) (Also possible in exposure to low pressure, as at altitude) *Repetitive dives are frequently involved.	Sudden onset during or very shortly after 1. Ascent, even from very shallow depth 2. Decompression from any increased pressure 3. Any accident or procedure that could permit gas to enter circulation
Proximate Cause	Usual. Diving or hyperbaric exposure beyond no decompression limits and without proper decompression stops Occasional: 1. Dive or pressure exposure within "no decompression limits" or with appropriate decompression stops 2. Low-pressure exposure, as in loss of cabin pressure in aircraft at altitude	Usual. Breath holding or airway obstruction during ascent or reduction of pressure Other. Entry of free gas into cardiovascular system during heart surgery or other medical/surgical procedure
Mechanism	Excess dissolved gas forms bubbles in blood or tissues upon reduction of external pressure. Bubbles produce local mechanical effects or circulatory impairment.	Usual. Overinflation of lungs causes entry of free gas into pulmonary vessels followed by embolization of the brain. Other. Pulmonary, cardiac, or systemic circulatory obstruction by free gas from any source.
Immediate Management	Essential emergency care as required (CPR, etc.) 100% oxygen by close-fitting mask Trendelenburg position, if feasible (*especially for suspected gas embolism*) Transportation to nearest suitable chamber Fluids orally, if conscious; otherwise intravenously	

Modified from *The Merck Manual of Diagnosis and Therapy*, Edition 15, p. 2379, edited by Robert Berkow. Copyright 1987 by Merck & Co., Inc. Used with permission.

subsystems. For reasons stated in par. 10-4, hydraulic systems usually are safer than pneumatic ones.

Pressure vessels generally will be safe if they are developed in accordance with the applicable American Society of Mechanical Engineers (ASME) code. The adequacy of the design and the manufacture should be verified by pressure testing. In "proof pressure" testing, the vessel is subjected to a pressure above the maximum expected operating pressure (MEOP) but below the yield point of the vessel. Thus a vessel tested this way can be used again. Vessels in service can be proof pressure tested to determine whether they are still safe.

The "burst pressure" test stresses a vessel until it begins to leak, which may occur at a pressure beyond the yield point of the material. Such vessels must then be discarded. Usually, a sample from a lot will be burst pressure tested to determine the actual burst pressure and the manner in which the vessel bursts. For example, does it rupture catastrophically and produce lethal fragments, or does it merely develop a crack and leak?

10-4.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

The safety criteria that follow are taken from MIL-STD-1522 (Ref. 20) and military specifications MIL-H-5440 (Ref. 21) and MIL-P-5518 (Ref. 22) for pneumatic and hydraulic pressurized subsystems. These are the principal safety design criteria for pressure systems, but they are by no means complete. A detailed listing of all pertinent safety criteria and background safety requirements for pressurized systems would be too voluminous to include in this handbook. Additional source documents are listed at the end of this paragraph.

1. Any pressure system that will operate where operators are normally present shall be designed with a minimum calculated safety factor—ratio of ultimate strength of the material to the allowable stress—of no less than 4.0 to 1.

2. When limited personnel access is required adjacent to pressurized tanks, the minimum acceptable safety factor—ratio of design burst pressure to maximum expected operating pressure—will be 2.0 to 1. If lower safety factors are employed, the tanks will be remotely pressurized and no personnel will be allowed access when the tanks are pressurized. Consult the applicable portions of the American Society of Mechanical Engineers code for specific situations and their safety criteria.

3. A 4 to 1 safety factor—ratio of design burst pressure to maximum expected operating pressure—for lines, tubes, fittings, and other components (valves, etc.) is the minimum acceptable.

4. Filters will be incorporated into each fluid system to protect safety-critical components by removing particulate matter that could be introduced into the system during filling or generated during operation and storage.

5. A filter will also be located at the last possible point before any critical item that could be damaged or that could fail because of plugging, jamming, or other adverse effect of particulate contamination.

6. Lines and connections will be designed so that cross connections cannot be made—between two different circuits, to other than the correct fitting on a subassembly, or in any but the proper manner—if an erroneous connection could result in an accident.

7. Protection against overpressure will be provided by the most suitable of one or a combination of the following devices or methods:

a. Direct, spring-loaded safety or safety relief valves

b. Indirectly operated safety or safety relief valves, such as pilot-operated valves

c. Rupture disks

d. Flow paths or vents that open, directly or indirectly, to the atmosphere

8. Each system equipped with a reducing and regulating device—to provide a pressure lower than that at the pressure source—will either

a. Be designed to withstand and operate under the full pressure throughout the entire system, or

b. Have an adequate relief valve installed downstream of the reducing and regulating device if full pressure would be detrimental or dangerous. This relief valve may be incorporated into the same housing as the reducing device, provided the relief valve mechanism is independent of the mechanism of the pressure reducer. The upstream working pressure will not exceed 75% of the maximum pressure for which the regulating device is designed.

9. Where heat absorption or temperature increase can cause an increase in pressure in a vessel or between two locked up components, means will be provided to prevent the pressure from exceeding 110% of the designed operating pressure.

10. Lines will be designed so that undesirable accumulations of moisture or other liquid will drain to reservoirs or to points at which it can be removed from the system.

11. Lines containing flammable, toxic, asphyxiating, or corrosive fluids will not be routed through enclosed inhabited spaces.

12. All direct-pressure readout gages will have shatterproof glass or plastic faces and blowout plugs.

13. Any component whose orientation is critical for safe operation of a pressure system will be of a type which cannot be installed other than correctly. This may be done by such means as different size connectors, asymmetrical designs, or use of indexing pins or keys.

14. Provisions will be incorporated for expansion and contraction in all metal piping. Semiloops for this purpose will be designed for movement in one plane only to eliminate any twisting motion. Straight-line connec-

tions will be avoided except where expansion joints are provided. In conjunction with expansion joints, the following features will also be provided:

    a. Anchors to eliminate stresses on the equipment being interconnected

    b. Guides to direct movement into the expansion joint

    c. A support to prevent the weight of the expansion joint from bending the line.

    15. Lines will be permanently marked in conspicuous locations to indicate the function served and the direction of flow. Markings will be placed where lines enter and emerge from closed compartments; they will be repeated at intervals to permit easy tracing.

The United States Code of Federal Regulations (Ref. 23) contains safety criteria for all types of pressurized containers and materials that may be transported in public carrier, vehicles, boats, and aircraft. Specific material transporting requirements are too voluminous to reproduce here and should be obtained by reference to the complete transportation section of the code.

The documents issued by Department of Defense agencies that contain safety provisions and detailed safety criteria for pressure subsystems are almost all written for aircraft and large missile systems. Although not initially issued for application to most Army equipment, the safety provisions of some of these documents can be used beneficially with minor adaptation. They include

    a. MIL-STD-454, *Standard General Requirements for Electronic Equipment*, Req. 1, par. 8.1. (Although this document primarily specifies the electrical safety criteria for electronic equipment, the general safety requirements of par. 3.3 (fail-safe), par. 4.0 (safety equal to or better than OSHA requirements), and par. 10.2 (safety from gases or fumes) are equally applicable to pressure subsystems.)

    b. MIL-STD-1247, *Marking, Functions and Hazard Designations of Hose, Pipe, and Tube Lines for Aircraft, Missile, and Space Systems*

    c. MIL-STD-1365, *General Design Criteria for Handling Equipment Associated With Weapons and Weapons Systems*

    d. MIL-P-8564, *Pneumatic System Components, Aeronautical, General Specifications for*

    e. MIL-H-8775, *Hydraulic System Components, Aircraft and Missiles, General Specifications for*

    f. NASA JSC 11123, *Space Transportation Systems Payload Safety Guidelines Handbook*, Lyndon B. Johnson Space Center, July 1976

    g. AFSC Design Handbook 1-6, *System Safety*, Design Note 3G2

    h. *ASME Boiler and Unfired Pressure Vessel Code*, Section VIII, American Society of Mechanical Engineers

    i. Air Force Technical Order 00-25-223, *Integrated Pressure Systems and Components (Portable and Installed)*

    j. *General Industry—OSHA Safety and Health Standards*, OSHA 2206 (29 CFR 1910) US Department of Labor.

10-5 TOXICITY

Toxicity is a relative term; it specifies the degree of hazard to humans posed by each type of injurious chemical. Since toxicity is a problem of organic impairment in humans, it constitutes a hazard only to personnel, not to equipment. A material is considered toxic if, in small amounts, it can produce an injurious effect on the average, normal human adult. This definition specifically ignores the possibility of an individual's peculiar, unusual susceptibility (allergy) to a particular substance (allergen). A substance is considered an allergen if small amounts will not injure the average person but will adversely affect certain people. Such allergic reactions by a few people have been reported for almost every commonly known material. Allergic reactions not only present a very real problem to manufacturers of consumable products but also have made it very difficult to determine precisely the dosages of toxicants that will cause injury to the normal adult.

Other factors that affect the determination of allowable dosages of toxic materials for the normal population are size and duration of dose (exposure), whether the toxicant is cumulative, rate of absorption, temperature, route of entry into the body, and physical condition of the affected person. Generally, the higher the toxicity rate of absorption and the higher the temperature, the more rapid the onset of injury will be. It is extremely difficult, however, to predict the exact toxicity level of a particular substance for a particular individual.

There are several ways to group toxic materials. Here they will be categorized by type of deleterious effect upon the body and within each category—systemic toxins, asphyxiants, and irritants—by the physical form of the toxicant, i.e., particulate matter or liquid.

Systemic toxins are those that cause biological damage after entering the body. For convenience, systemic poisons will refer only to those agents that enter and are carried by the bloodstream to the internal organs they affect. Asphyxiants include only those substances that interfere with the respiratory process and the transfer of oxygen into the bloodstream. Irritants are those substances that damage or destroy human tissue at the point of contact. If an irritant is inhaled or ingested, it will attack the body's internal soft tissue.

One of the most important factors determining the effects of a toxic substance is the route by which it enters the body. Solids or liquids most commonly enter the body through the mouth, and gaseous substances usually enter through the mouth and nose. The digestive system provides a good defense against substances entering through the mouth because digestion is a process of decomposi-

tion by chemical means. Some toxic substances that enter the digestive system will be rendered harmless by chemical interaction with the stomach acids and enzymes or with the food undergoing digestion. This process, however, can also work in reverse, i.e., transforming an entering substance into a toxicant as happens with carcinogens. (Carcinogens must be activated by enzymes in the liver before they become cancer-causing materials.)

The respiratory system has no such chemical defenses against toxic substances and only minor mechanical defenses. Its chief defense is against particulate matter picked up by the hairs in the nostrils, the mucous membranes, and the trachea. Once a toxic substance has entered the lungs, the body is quite defenseless against it. For this reason the respiratory system is the most dangerous route of entry for toxic materials. Accordingly, gaseous toxicants are the most dangerous.

Ref. 24 classifies particulate matter carried as aerosols—atomized particles of a substance suspended in air—into four classes:

1. *Smokes*. Usually solid particles of carbon, which result from the burning of carbonaceous material. Carbon smoke contains particles of about 0.01 micron $(0.4 \times 10^{-6}$ in.) that tend to coagulate or agglomerate rapidly into long, irregular filaments several microns in length.

2. *Dusts*. Solid particles ranging in size from 0.1 micron $(4 \times 10^{-6}$ in.) or less (haze) to the large particles associated with a sandstorm.

3. *Fogs*. Liquid droplets generated by atomization or condensation of volatile substances on minute nuclei. The size of these particles is often quite large and ranges from 4 to 40 microns $(1.6 \times 10^{-4}$ to 16×10^{-4} in.), as in a natural-water fog.

4. *Fumes*. Solid particles generally produced by sublimation, combustion, or condensation—usually sized between 0.05 and 0.5 micron $(2 \times 10^{-6}$ and 20×10^{-6} in.). Fumes can also be produced by arcing at high temperatures, as in arc welding.

Liquid, solid, and gas toxicants may also enter the body through any open wounds in the skin. They may also enter by injection if propelled at high velocity. High-pressure paint spray or a high-pressure jet of compressed gas (air) are examples. Some toxicants, e.g., tetraethyl lead, can be absorbed through normal unblemished skin and are particularly dangerous because their entry is totally unnoticed.

Systemic poisons work in two ways: (1) they may interfere with the metabolic process and prevent the use of oxygen by the body in a normal manner or (2) they may prevent certain organs from carrying out their normal functions. A particular type of systemic poison will only attack certain specific organs even though it is carried to all parts of the body by the bloodstream.

Irritants attack the tissue at the point of contact by dilating the capillaries and increasing their permeability, so that fluid passes from the blood into the tissue. This causes redness, swelling, and an increase in skin temperature. The increased fluid pressure on nerve endings causes pain. Very strong irritants will cause the fluid to collect in body tissue in such large amounts that blisters form.

An irritant may be a gas, a liquid, or very fine particles. Even a small amount of irritant may cause extensive damage, depending on which area is attacked and the type of irritant. In the respiratory tract an irritant may function by chemical or mechanical (abrasive) means. In the upper tract, the irritant may cause inflammation and pain or tissue destruction. In the lower tract it may cause pulmonary edema (accumulation of fluid in the lungs), which blocks the passage of air. The end effect of this event is suffocation. Some irritants are not toxic when dry but become toxic in the presence of moisture. These will cause irritation in the respiratory tract, as well as in the digestive system, when the irritant contacts the moist mucous membranes.

Asphyxiants can be classified as either simple or chemical. Simple asphyxiants dilute or block the inspiration of air, so that the lungs cannot supply the blood with sufficient oxygen. Chemical asphyxiants enter into and combine with the hemoglobin in the blood, so that the blood does not properly absorb oxygen from the lungs. Ref. 25 states, "A number of gases and vapors, when present in high concentrations of air, act primarily as simple asphyxiants without other significant physiologic effects. A Threshold Limit Value (TLV) may not be recommended for each simple asphyxiant because the limiting factor is the available oxygen. The minimal oxygen content should be 18% by volume under normal atmospheric pressure (equivalent to a partial pressure, pO_2 of 135 mm Hg). Atmospheres deficient in O_2 do not provide adequate warning and most simple asphyxiants are odorless. Several simple asphyxiants present an explosion hazard. Account should be taken of this factor in limiting the concentration of the asphyxiant.". Specific examples of asphyxiants are acetylene*, argon, ethane*, ethylene*, helium, hydrogen*, methane*, neon, propane*, and propylene*. (Substances indicated by an asterisk are also flammable and explosive.)

Hemoglobin (Hb) has a preference for carbon monoxide (CO) over oxygen, and even small amounts of this CO toxicant will be absorbed by the blood. Fig. 10-12 (Ref. 16) shows the effects of CO on man as functions of concentration and exposure time. The solid lines are the exposure limits set by the military services for aircraft interiors. The level marked at 0.005% CO (50 ppm) is the current TLV for 8-h-per-day exposure in industry. The point marked at 0.04% CO (400 ppm) is the current short-term exposure limit (STEL) for 15 min or less.
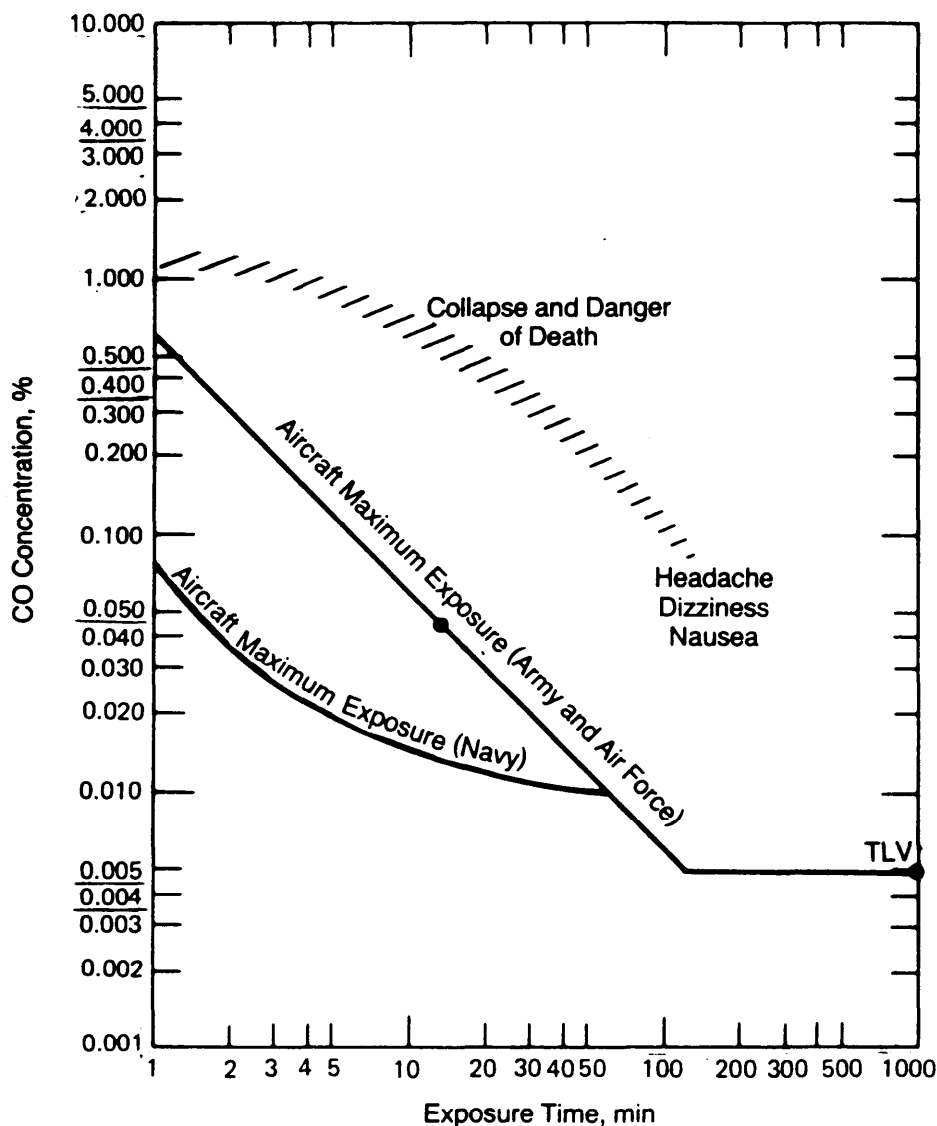
Figure 10-12. Effects of Breathing Carbon Monoxide (Ref. 16)

When the blood lacks enough oxygen to sustain body functions, the condition is known as hypoxia. One of its first effects on the body is a decrease in mental capabilities. The brain receives only 20% of the total blood supply but requires 80% of the oxygen supplied by the blood; therefore, the brain reacts most rapidly to the effects of hypoxia. Irreversible damage *may* occur if the oxygen supply to the brain is interrupted for longer than 5 min, although there have been exceptions to this. There is no positive method to forecast for an individual the precise interval without oxygen at which brain damage will occur. Lesser degrees of hypoxia cause increases in reaction time, loss of ability to concentrate, and a state of euphoria. This last effect is the most dangerous because a person has no awareness of the existing problem. An equipment operator suffering from the effects of hypoxia can believe that everything is normal when, in fact, he is making errors or the equipment is failing.

One class of toxic substances, i.e., anesthetics, causes loss of sensation; the effects of anesthetics may be either local or general. They depress the nervous system and cause loss of consciousness with its associated dangers. The greatest danger of an anesthetic, however, is that it may interfere with involuntary muscular reaction and cause cessation of breathing. Novocain (local) and chloroform (general) are common examples of anesthetics. Both are very highly flammable and, in closed areas, are explosive.

Neurotoxins depress or stimulate the central nervous system and the brain. They may be selective or they may act on the entire system; however, increasing amounts of either type will generally affect all the organs eventually. Depending on the type of toxicants, an operator can exhibit drowsiness, inability to concentrate, euphoria, apathy, dimness of vision, and rapid flow of uncontrolled thought (Ref. 26). Depressants generally act as stimu-

lants before beginning to depress the nervous system. Then they cause labored breathing, a bluish discoloration of the skin due to poor oxygenation of the blood, and eventual loss of consciousness. Stimulants, on the other hand, accelerate the bodily functions and are evidenced by excitement, rapid pulse, and, in extreme cases, jerking of the muscles, disorganized vision, and deliriums. Alcohol, often considered a stimulant, is an example of a depressant. Caffeine is a stimulant. All these effects of neurotoxins are undesirable in equipment operators. Whether released from the materials and functioning of the equipment itself or acquired from external, unrelated sources, these neurotoxins are to be avoided.

Hypnotic toxicants affect the central nervous system in a limited way by inducing drowsiness and sleep. The danger of these substances is the danger inherent in falling asleep at a critical time, such as when operating a machine or driving. All barbiturates are hypnotics as are certain other drugs prescribed for alleviation of cold symptoms and allergies.

Toxic substances that cause cancer are classed as carcinogens. This classification of toxicants has only recently come into common usage. Most of the substances presently considered carcinogens were discovered to be such only after prolonged, uncontrolled use. Personnel exposed to or using these substances experienced a higher than normal occurrence of cancer. Other carcinogens have been discovered by laboratory tests on animals. The exact effect of any suspected carcinogen is obviously a complex subject. When designers must use materials from any list of suspected carcinogens, they are advised to seek expert medical advice. Each year the list of suspected or known carcinogens grows larger and includes many substances commonly used in industry for years. For example, asbestos has been known to cause lung irritation and asbestosis for quite some time but has only recently been shown to cause cancer. Ref. 25 lists substances in industrial use that have proven carcinogenic in man or have induced cancer in animals under appropriate experimental conditions. The list takes two forms, i.e., (1) those carcinogens for which TLVs have been assigned and (2) those for which environmental conditions have not been sufficiently defined to assign a TLV. Ref. 27 lists 14 chemicals—known to cause cancer in humans or in two species of animals—by their full chemical names, trade or common names, frequent and usual uses, and by the specific cancer-related hazard each presents.

Injuries resulting from the mechanisms of some toxicants, e.g, carcinogens, are sometimes delayed for long periods of time. Others have effects that are delayed for lesser, but still extended, periods. An example of such a systemic toxicant is carbon tetrachloride, which damages the liver and kidneys.

Corrosives are a special class of irritant. Generally, they are powerful acids such as sulphuric, nitric, hydrochloric,

and hydrofluoric. They destroy the skin and open an entry into the underlying tissue. Once the protective barrier of the skin has been breached, the corrosive agent attacks the tissue at an ever-increasing pace. Finally, some of these substances can enter the bloodstream and act as systemic poisons.

Some success has been achieved in establishing safe levels of toxicants for adult humans. This knowledge can greatly assist the designer in his work; however, the designer must still have an understanding of the physiological processes of absorption, the effects that can be produced, and safeguards to prevent injury. Because the tolerances of individuals to a particular substance will vary, the permissible level to which anyone may be subjected is generally far below the minimum level considered injurious to most persons. Even so, improved research continues to discover that substances are more injurious than had been previously considered. Accordingly, permissible levels may have been excessively high and, therefore, will not provide protection to everyone.

There are three commonly used methods of expressing measurements of toxicity:

1. *Time Concentration Factor C_t.* The factor is concerned with toxicants that enter the respiratory system and represents a specific response by normal subjects to a given vapor concentration of the toxicant over a specific exposure time.

2. *Dosage Factor D_t.* This factor is a measurement of toxicants that enter through the skin or mouth, i.e., it measures the quantity of liquid or solid that must be ingested into (or in contact with) a normal subject's body of given weight to produce a given reaction. Both C_t and D_t indicators are qualified as to whether they represent lethal (L) doses or incapacitating (I) doses. Each of these measures is derived from laboratory testing of animals and allows only rough approximations of human effects.

3. *Incapacitating Concentration Factor IC_{50}.* This factor indicates the time concentration of a vapor that will incapacitate 50% of the subjects. For example, an IC_{50} value for a particular vapor might be expressed as 1800 mg/min·m³, i.e., milligrams of toxicant per minute per cubic meter of ambient air.

TLVs indicate the average concentration of a toxicant that can be tolerated continuously without injury during the 40-h week spanning a working lifetime. The values are expressed in milligrams per cubic meter (mg/m³) and in parts per million (ppm). TLVs are concerned primarily with toxicants that enter the respiratory system.

10-5.1 TOLERANCE AND SAFE EXPOSURE LIMITS

It can be seen from Fig. 10-12 (Ref. 16) that the TLV of 0.005% for CO is less than that which can generate adverse effects (headaches, dizziness, nausea) and far less than that which can cause collapse and danger of death.

As previously indicated, the TLVs are based on a 40-h week over a lifetime.

Another measure of toxicity is the short-term exposure limit (STEL). This indicates the vapor concentration to which a normal person can be exposed for up to 15 min without injury. The STEL establishes safe vapor concentration levels for no more than four 15-min exposures per day with 60 min between exposure periods and provided that the daily TLV time-weighted average is not exceeded. Note from Fig. 10-12 that the STEL of 0.045% CO is nine times the TLV. For some substances a TLV-C (ceiling) has been established. This is a concentration that should not be exceeded even instantaneously (Ref. 25).

TLVs are established by the American Conference of Governmental Industrial Hygienists (ACGIH) based on analyses of experience data, which appear to be reliable, and on laboratory tests (Ref. 25). TLVs were listed in TB MED 265 (Ref. 28). However, because the lists are extensive and frequently changed as additional information becomes available, the latest list issued by the ACGIH should be consulted. OSHA also publishes lists of materials considered to be carcinogens, which should be consulted (Ref. 29).

10-5.2 POTENTIAL HAZARD SOURCES

The sources of toxic hazards in Army systems have multiplied with the advent of missiles, rockets, jet engines, and ever-increasing numbers of self-propelled equipment for the mobile Army of today. CO from the exhaust of internal combustion engines continues to be a toxic problem in the Army; however, many other systems, subsystems, and assemblies generate toxic agents.

Ordnance for chemical warfare is designed to produce various toxic reactions that range from mild and temporary to long-lasting and fatal. Since this is a specialized activity, designers developing subsystems that interface with chemical ordnance must use expert assistance from Army chemical ordnance personnel to solve the related design problems.

When missiles are fired, the missile propellants produce toxic combustion products. The chemical composition of the gaseous products formed by the combustion of propellant fuels and oxidizers depends on several factors. Among these are the types and proportions of the reactants used, the presence of small amounts of stabilizers and inorganic materials often found in propellants, and the conditions under which combustion occurs. In addition, two or more of the combustion gases may react, depending upon the relative timing of their formation.

With sufficient data regarding the chemical composition of the propellant reactants and the conditions of combustion, such as the temperature, the major constituents of the combustion products can be predicted with a reasonable degree of accuracy. Thus the normal products of combustion of carbonaceous propellants and nitrate oxidizers will contain carbon monoxide, carbon dioxide, hydrogen, nitrogen, and oxides of nitrogen. Ammonia, methane, and nitrocarbons may be formed if the reaction is badly underoxidized. If the propellant contains sulfur, the combustion products may also include sulfur dioxide, sulfur, hydrogen sulfide, and sulfur trioxide. Propellants containing chlorine will produce hydrochloric acid and chlorine. At high temperatures of combustion, small amounts of inorganic materials in propellants form metal oxides, hydroxides, or halides. Above 2500°C (4530°F), highly reactive dissociation products combine to produce a variety of combustible and toxic gases.

In assessing the hazards associated with propellants and propelling charges, a prediction of the qualitative composition of the combustion products in a general way is a good beginning. Next, detailed studies of the combustion process should be made under actual conditions of use to evaluate the kind and degree of health hazard associated with exposure of personnel to the combustion products and to develop the appropriate protective measures when indicated. The designer should consider the contribution of each propellant material to the chemical composition of the combustion products. When performance requirements are balanced against the adverse effect of the toxic combustion products under the probable field conditions, the optimum propellant design can be developed. In some cases the analysis may indicate that operating personnel require respiratory protection.

The effectiveness of military protective masks against the "fumes"—nitrogen dioxide or nitrogen tetroxide—of red or white fuming nitric acid is affected by the concentration of the fumes and the duration of the exposure; consequently, the masks may not be adequate. Therefore, under emergency conditions in which personnel may be exposed to heavy concentrations of these fumes for long periods, exposed personnel should be provided with air- or oxygen-supplied respirators. Also military protective masks should not be used where there is risk of simultaneous exposures to the vapors of fuel and oxidizers because of the possibility of a hazardous reaction in the canister or cartridge of the mask.

Toxic hazard sources of lesser importance, but which must be considered by designers and analysts, include such substances and usages as

1. Solvents for cleaning many types of Army equipment
2. Chemical reactants for chemical lasers
3. Acids and alkalies for batteries
4. Refrigerants and coolants for cooling systems
5. Asbestos from vehicle brake shoes
6. Beryllium from high-temperature devices.

10-5.3 HAZARD CONTROL TECHNIQUES

Since the mobile Army moves and operates primarily with the aid of internal combustion engines, carbon monoxide—the principal toxic combustion product exhausted by the engine—must be recognized and controlled. The amount of carbon monoxide discharged through the engine exhaust is somewhat—but not to a practically effective degree—dependent on the design and adjustment of the engine. At present there is no practical design technique to eliminate this toxic hazard. The primary design method to control carbon monoxide pollution is to locate ventilation intake ducts far away from engine exhaust outlets in all Army equipment. Insofar as is possible, the equipment should be positioned so the prevailing wind will carry exhaust away from operating personnel. Vehicles with operating personnel in closed compartments should be provided with a means of closing the outside air intake ducts. Operating personnel can be protected positively by use of air- or oxygen-supplied respirators.

If a toxicant cannot be eliminated, its level can often be reduced with ventilating equipment. The ventilation of air-conditioned compartments is particularly important. To improve the effectiveness of air-conditioning, compartments are very often tightly sealed; this minimizes the natural flow of air and increases the possibility of retaining contaminants in the ventilated compartment. Further, the air intakes for ventilation or air-conditioning should not be located near sources of pollutants such as the exhaust of an engine or rocket motor. Gas masks or other breathing apparatus may be required when equipment design solutions are not possible.

When persons must wear protective equipment to enter a contaminated or toxic environment, respiratory protection should be provided by a self-contained breathing apparatus or, for long duration use, piped air equipment. Canister-type gas masks are the least reliable, have limited capacity, and are ineffective where there is an inadequate level of oxygen. In addition, some canisters will not remove certain types of toxic gases very well, such as carbon monoxide. For canister-type masks to be used safely, they should be approved by the National Institute of Occupational Safety and Health (NIOSH).

The guidance for physiological response of operators to CO exposure is given in Table 10-11 (Ref. 30). Since CO is most prevalent in the everyday Army environment, these values have been determined through various tests and experience data. Comparable tables for other combustion products may become available, but for the present designers should use the TLVs in the current annual list published by the American Conference of Governmental Industrial Hygienists (or reproduced in Army publications) (Ref. 25).

TABLE 10-11. PHYSIOLOGIC RESPONSE TO CO EXPOSURES IN HEALTHY SUBJECTS (0-50 ppm—NO APPRECIABLE EFFECT) (Ref. 30)

Carbon Monoxide Concentration in Air, ppm	Carboxyhemoglobin Saturation in Blood, %	Exposure Time	Symptoms
0-100	0-17		No appreciable effect except occasional slight tightness across forehead and slight flushing
200-300	23-30	5-6 h	Throbbing temporal headache, generalized weakness-dizziness, dimness of vision, nausea, vomiting
400-600	36-44	4-5 h	Same as above, with muscular incoordination and collapse
700-1000	47-53	3-4 h	Same as above, with increased pulse and respiration
1100-1500	55-60	1.5-3 h	Coma with intermittent convulsions and Cheyne-Stokes respiration
1600-2000	61-64	1-1.5 h	Same as above, with depressed heart action and respiration, possible death
5000-10,000	73-76	2-15 min	Death

10-5.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

When toxic hazards may exist, the following safety guidelines should be used for the design and operation of Army equipment:

1. Obtain the latest information on toxic characteristics of materials proposed for use in the equipment to be procured or designed.

2. Design the equipment to use, consistent with mission requirements, materials that will produce the least toxic hazard to operating personnel.

3. When possible, design the equipment with self-contained filtering systems to protect personnel from the toxic hazard produced by operation of the equipment.

4. In mobile equipment with enclosed operator compartments—such as tanks, self-propelled guns, and missile launchers—provide the capability to close the air intake ducts.

5. Provide complete information on toxic characteristics of the equipment to the activity responsible for preparation of the training materials and the operating and maintenance manuals.

10-6 VIBRATION

Vibration hazards may be divided into those that affect humans and those that cause equipment to degrade or fail. Audible vibration hazards, which include such effects as loss of hearing, will be dealt with separately in par. 10-7. Only the physiological and psychological hazards of vibration outside the audible range will be discussed in this paragraph.

Fig. 10-13 (Ref. 31) indicates some general human reactions to low-amplitude vibration. High-amplitude vibration can cause physical injury by impacts and other acceleration and deceleration effects described in par. 10-15. In addition, prolonged exposure of the hands and
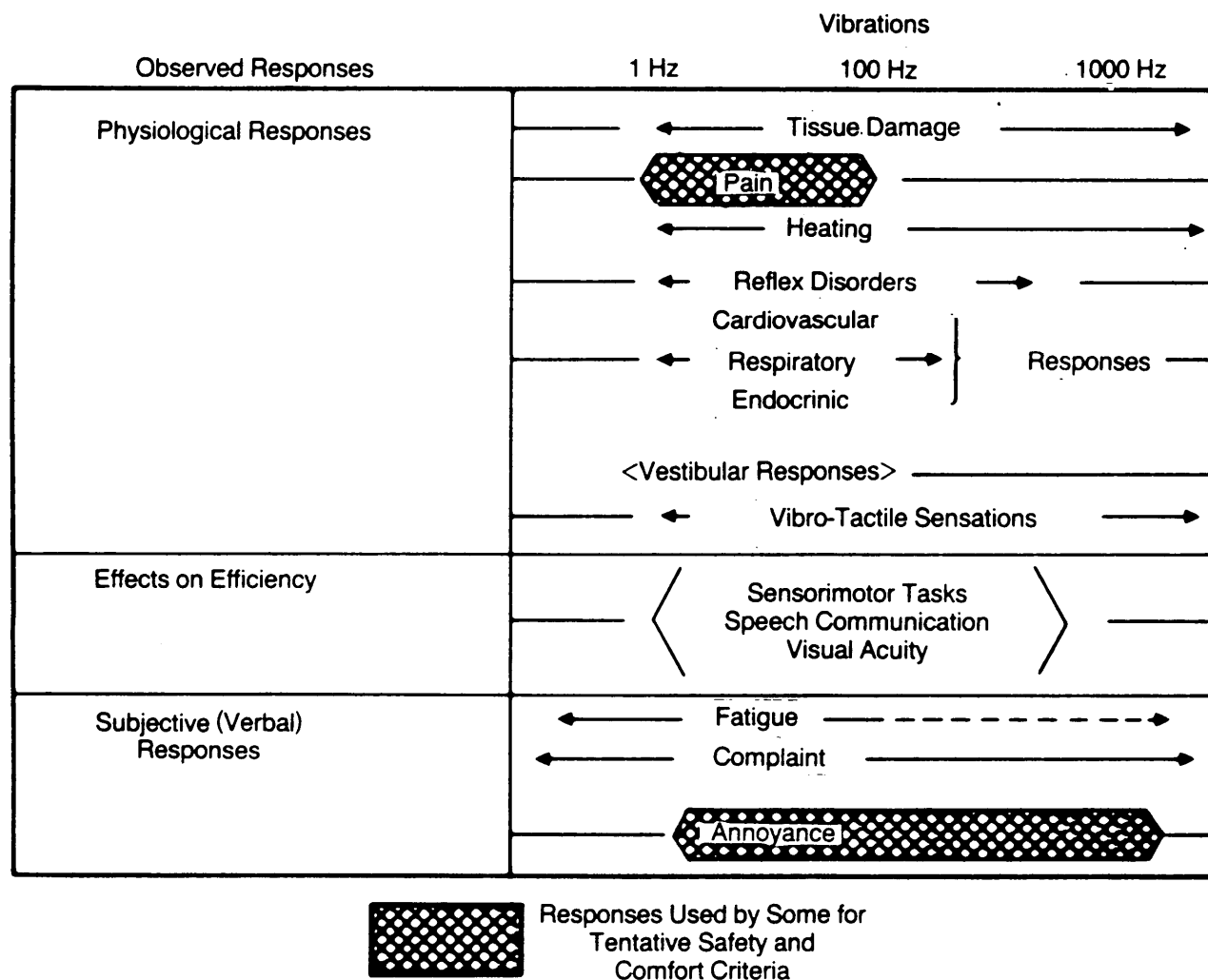
Figure 10-13. Human Reactions to Vibration (Ref. 31)

arms to vibration in certain frequency ranges will produce a phenomenon known as Raynaud's disease. The disease is characterized by blockage of blood vessels, which results in reduced blood flow. The symptoms—which affect the hands—are a loss of feeling, a sensation of coldness, and pale skin; all are due to the oxygen deficiency caused by decreased blood flow. The phenomenon seems to occur only to the hands when hands are subjected to vibrations produced by impact and vibrating tools operating in the range of 2000 to 3000 cycles per min and by hand-held grinding tools. Grinding tools generate the phenomenon when their rotational velocity produces vibrations in the range of 40 to 125 Hz, which may occur at various rpms. As yet there is little evidence that the same phenomenon would result if the feet were exposed to comparable vibrations—possibly because the feet are seldom subjected to this type of vibration. However, the rotor pedals in helicopters commonly produce vibrations that may well subject the feet to the 40- to 125-Hz vibration range. Until research or use factors prove otherwise, efforts should be made to avoid exposing the feet of helicopter pilots to the suspect vibrations.

Raynaud's phenomenon is an example of one injurious effect of vibration on a member of the body. Whole-body vibration—displacing organ systems and their supporting structures—can produce other injuries. The relative displacements are a function of the frequency, magnitude, and direction of excitation. Further, for a given type of excitation, the magnitude of the displacement is a function of the natural frequency and damping factor of the system and of coupling to the point of excitation. Other vibration effects—although not injurious—may be annoying, debilitating, or painful and may increase the tendency to commit errors and cause accidents. Table 10-12 (Ref. 32) lists these noninjurious effects. Ref. 32 also relates these responses to frequencies in the 1- to 10-Hz range with amplitudes of 5.8 to 445 mm (0.23 to 17.5 in.) and accelerations of 0.4 to 1.8 g.

Vibration can prevent a person from making fine adjustments to instruments or equipment or accurately manipulating controls. The source of the vibration may be in the equipment, the seat or floor supporting the operator, or may result from a combination of both. Air-conditioning units, rotating or oscillating electromechanical equipment, and power-generating equipment are possible sources of vibration. In Army aircraft, vibration is caused by the on-board machinery and the variable smooth-to-turbulent air through which the aircraft passes. In mobile combat equipment, vibration can be caused by on-board machinery, operations in rough terrain, missile launching, artillery firing, or exploding ordnance.

In equipment operation the controls may be vibrating so badly that the operator has difficulty maintaining a grasp upon them. Conversely, the operator may be

vibrating so badly he has difficulty maintaining his position relative to the controls and must rely heavily upon his grasp of the controls to maintain his position. The designer must consider this possibility and provide some means—such as shock-mounted seats with seat and shoulder belts—to steady the operator. Human factors engineering must also consider the best designs to facilitate optimum operator performance in situations—such as combat, adverse weather, and rough terrain—that involve large-amplitude vibration.

Instruments may vibrate so severely that they cannot be read accurately or cannot produce accurate readings. This situation can be aggravated if the operator's work platform is also vibrating independently. The end result is degraded performance by the operator. The designer can relieve this situation by providing shock-mounted and damped instrument panels or individually shock-mounted and damped instruments.

Constant exposure of the operator to vibration can be a highly distracting force. This distraction can be manifested either physiologically or psychologically. High-frequency vibration can cause limbs and outer extremities to become numb. Low-frequency vibrations can cause rapid onset of fatigue due to constant tensing of the body muscles against upsetting influences. These debilitating effects can result in psychological dysfunction in the form of annoyance and diversion of attention.

Prolonged exposure to vibration can lead to bursitis and arthritis. Very high-frequency vibration (above 10 kHz)—indiscernible by normal feel and outside the audible field—is becoming more suspect everyday as the cause of physical and mental debilitation, of which the exact mechanics are not yet fully understood. The debilitating effect may be otherwise unexplained tiredness or mental confusion or both.

Exposure of equipment to vibration can cause fatigue and eventual failure from breakage. The most widespread problem of this type is metal fatigue. Metal fatigue results from the progressive unbonding of atoms within the crystal structure of the metal due to the shear effect of flexing loads. These same results may be produced by a wide variety of vibration frequencies and amplitudes. Metal parts with large, unsuspended masses that are subjected to vibration are highly susceptible to metal fatigue. The area that fails most frequently is at the point of attachment because that portion of the part cannot vibrate at the same frequency or amplitude as the rest of the mass; the resulting flexure causes shear loads. Vibration will also cause parts made of fiberglass or polymer-resin plastics to fail because the material becomes brittle.

Vibration can cause equipment to oscillate such that adjoining parts will contact one another. The most common result of mild but continuous contact is abrasion. Violent contact may result in immediate or eventual breakage of one or both of the parts. Another result may

TABLE 10-12. NONINJURIOUS VIBRATION EFFECTS ON HUMANS (Ref. 32)

HEAD-NECK

Head Sensations	Vibration or "tight" sensation of facial skin
Pharynx	Pharyngeal tug or "lump in throat"
Jaw	Sensation of vibration
Speech	Lower frequencies secondarily affected due to reactions of thorax and abdomen; high frequencies due to superimposed transmitted vibrations to laryngeal tissues and possibly mainstream bronchi

THORAX

Respiration	Decreased ability to perform physiological respiratory movements of the thoracic cage due to superimposed forces from oscillating platform
Dyspnea	Actual air hunger
Valsalva	Partial or complete closure of glottis resulting in increased intrathoracic and intraabdominal pressure
Pain	Dull-to-severe pain of the pericardium occasionally radiating to the sternum; no other radiations; pain subsiding immediately after cessation of vibration

ABDOMEN

Voluntary Abdominal Musculature Contraction	Degree of contraction or "bearing down"
Pain	Usually periumbilical with tendency to radiate to right lower quadrant

SKELETAL MUSCULATURE

Skeletal Musculature	Sensation of "muscle tightness" or possibly increased muscle tone primarily of the lower extremities, dorsum, and neck
Voluntary Muscle Contraction of Extremities	Muscular contraction in an effort to counteract movements of oscillating platform
Lumbosacral Pain	Dull-to-severe pain at midline with bilateral radiation; pain subsiding immediately after cessation of vibration

PELVIC-PERINEAL COMPLEX

Micturate (Urge)	Mechanical stimulation of bladder neck and proximal portion of urethra
Defecate (Urge)	Mechanical stimulation of distal portion of sigmoid colon and rectum

GENERAL DISCOMFORT

	Overall estimation of each frequency ridden

be deformation of the parts. If the parts are articulated, they may bind intermittently. A complicating factor is that the parts may vibrate in the unacceptable fashion only at certain times when the equipment is in a particular phase of operation, i.e., exhibits a frequency dependence. The amplitude of the vibration is greatly increased when the vibrating machinery is vibrating at the natural frequency of vibration of the major mechanical subsystem to which it is connected or mounted.

Vibration may be the result of articulation, rotation, or oscillation in a piece of equipment. Internal vibration may become a problem only because of its mounting. This usually occurs because the mounting is too rigid, but it can also result from too flexible a mount. In the early configurations of a helicopter model, the engine, transmission, and rotor hub were assembled into a single rigid unit. This unit was mounted in a framework that, in turn, was secured to the structure of the helicopter with moderately flexible mounts. Cracks immediately began to appear in the engine framework. Each time the framework was strengthened, the strengthened member would crack in a new location. The problem was finally

solved by increasing the flexibility of the mounts joining the engine framework to the aircraft structure, and this solution transmitted less vibration to the aircraft structure.

Transmitted vibrations—usually resulting from connections that are too rigid—are most difficult to deal with when both units vibrate independently and each is mounted on an independent surface. As with internal vibration problems, the source of transmitted vibration may be rotation, articulation, oscillation, or a combination of these. Sometimes transmitted vibration can be corrected by the reorientation of a component.

Some of the more common sources of vibration internal to equipment are

1. Unbalanced rotating units
2. Bent shafts on rotating units
3. Impact of moving parts
4. Hydraulic shock
5. Pulsation of high-velocity air in ducts
6. Gear slippage
7. Belt slippage
8. Flat spots on bearings or wheels.

Some common causes of induced vibration are

1. Misalignment of driven and driving equipment
2. Impact between oscillating or articulating parts
3. Inflexibility of connections between equipment or components
4. Oscillations of thin panels or surfaces in jet streams.

The medium through which vibration is transmitted has a major effect on the transmission. All liquids are excellent vibration transmitters. Vibration is transmitted more readily through solids and liquids than through air. The physical form and composition of the solid affects the transmission of vibration. Steel transmits vibration better than lead, concrete better than earth, and impacted earth better than loose earth.

The major hazard to machinery from vibration is structural failure that results in loss of the equipment. The failure may be sudden and catastrophic, such as the loss of a rotor blade on a helicopter. Alternatively, the loss may be progressive; one failure causes increased loading on another part whereupon that part fails or causes other parts to fail. An example would be a bolt failing from fatigue and falling into a transmission, causing its failure and the subsequent loss of the entire machine. Continuous vibration may cause fatigue in electromechanical equipment and may result in excessive wear of joined parts with bearing surfaces, maladjustment of parts with spring tension, intermittent operation, and breakage of electrical wires from their terminals.

Vibration may cause unsecured items to move about on the vibrating surface and fall over and break. Eventually, items may fall off the edge and break or strike a person and cause an injury.

10-6.1 TOLERANCE AND SAFE EXPOSURE LIMITS

Fig. 10-14 (Ref. 33) indicates vibration frequencies that can be tolerated by a seated person. The actual safe exposure limits would necessarily be less than the values shown to provide a safety factor and to account for differences in individual tolerances between persons.

Fig. 10-14 illustrates schematically a number of tolerance criteria for vibration. The four shaded zones represent (1) the threshold of perception, (2) the unpleasant area of vibration, (3) the limits of voluntary exposure, unprotected, for 5 to 20 min, and (4) the voluntary tolerance limits for subjects with lap belt and shoulder harness exposed for 3 min, 1 min, and less than 1 min. Above this upper limit, minor injuries occur, depending on exposure time. At the top of the figure the voluntary tolerance curve for impact is plotted, which may be considered half-cycle vibration of large magnitude. The conventional way of measuring durations t and amplitudes A is shown in the small diagrams at the left of Fig. 10-14.

Limits of equipment vibration are established in specifications. The numerical values of these limits generally depend on the type of equipment and the degree of precision required to operate the equipment satisfactorily. For example, a mobile repair shop for electronic equip-
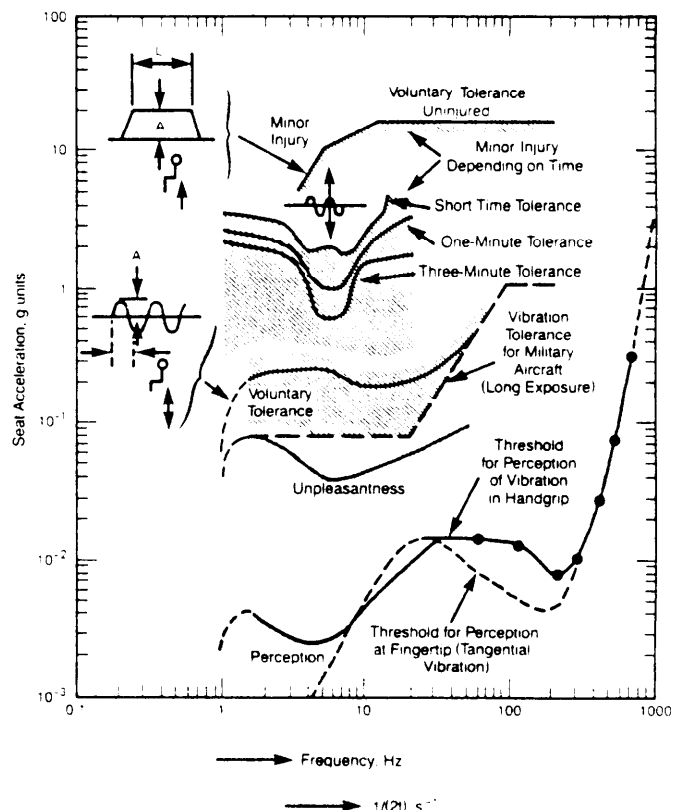
Figure 10-14. Criteria for Vibration Tolerance in Longitudinal Axis While Seated (Ref. 33)

ment will require lower levels of vibration than an armored personnel carrier. A vibration severity chart for developing vibration specifications is presented in Fig. 10-15 (Ref. 33). This figure can also be used to evaluate vibration characteristics during tests of prototypes or production models.

10-6.2 POTENTIAL HAZARD SOURCES

Tables 10-13 (Ref. 34) and 10-14 (Ref. 34) list some characteristics and causes, respectively, of vibration in equipment. In addition, vibration can be caused by environmental conditions not indicated in these tables, e.g., by high winds. Vibrations can be generated by the passage of aircraft through the air or by the motion of ground vehicles on rough terrain. Vibration results when fluids, passing through pipes at high velocity, strike inner surfaces of the pipes or suddenly stop flowing because of a closed valve (water hammer).

10-6.3 HAZARD CONTROL TECHNIQUES

Design strategies to avoid vibration can be divided into three major categories:

1. Strategies and techniques to avoid vibration
2. Techniques to isolate vibration from personnel, other components, or other equipment
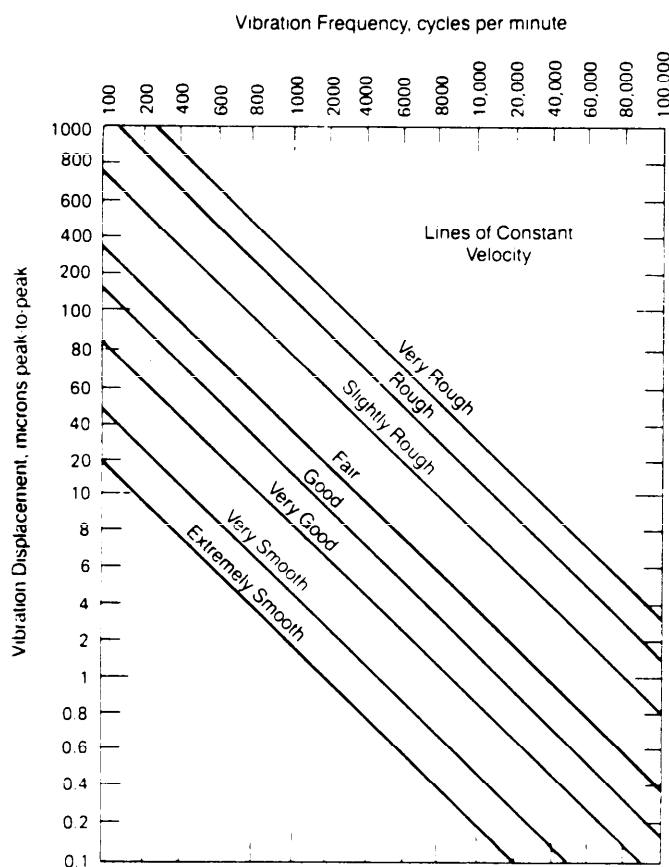
Figure 10-15. General Machinery Vibration Severity (Ref. 33)

3. Techniques to control (reduce) vibration at its source.

The designer must be always alert to the sources of vibration and avoid designs that produce these sources. This is very difficult to accomplish when designing machinery because the sources of vibration are rotational, oscillatory, or articulatory velocities, and most machines generate at least one of these velocities. Choices, however, often can be made among types of designs to accomplish the same end purpose. For example, jet engines and reciprocating gasoline engines perform the same end task, but jet engines have no oscillating parts and produce far different spectrums of vibration. Within the jet engine category, turbojet and propjet engines also accomplish the same end result with far different vibration spectrums. Also hydraulic transmission systems accomplish the same task as gears, cables, and pulleys, and both of these differ from electrical wires and solenoids and motors; yet these systems have greatly varying vibration characteristics.

If vibration cannot be eliminated, it must be isolated by means of carefully controlled equipment design and installation. A good start is the elimination of as many moving parts as possible from the design. Closely controlled fabrication of oscillating parts and consideration of mass distribution will reduce much of the vibration. Thoughtful selection of the mounts and dampers will reduce or eliminate the residual vibration.

If vibration cannot be eliminated from a particular component, that component should be isolated as much as possible to prevent propagation of the vibration to another component or the major equipment. When this cannot be accomplished, other critical components should be isolated from the vibration of the major structure. The first choice for interfaces between moving parts should be fluid couplings; the second choice, pneumatic couplings; and the third choice, precisely aligned, universally flexible, mechanical couplings. Dampers should be used whenever necessary but only as a last resort.

Crew and operator stations should be isolated from vibrating equipment. Controls to vibrating machinery can be linked hydraulically, pneumatically, or electrically, rather than mechanically. Mechanically linked controls should incorporate vibration-isolating features such as damped cables or rods.

Instruments that cannot be located independently of vibrating equipment should be shock mounted or damped. In addition, the instruments can be designed to provide the required information in high-vibration environments. In such instruments, the pointer increments between numbers can be made larger or digital readouts can be incorporated. When incremental readouts are not required, limit lights can be used.

To eliminate the need for precise adjustments in high-vibration environments, consideration should be given to automatic systems. Controls can be eliminated by using

TABLE 10-13. CHARACTERISTICS OF COMMON VIBRATION CONDITIONS (Ref. 34)

Vibration Cause	Vibration Frequency (relative to machine rpm)	Characteristics
Unbalance	Same	The most common cause of vibration is unbalance. It occurs when the center of mass of an object is not also its center of rotation. The apparent presence of a "heavy spot" causes forces to be applied, which causes a vibration whose amplitude is directly proportional to the amount of unbalance and whose frequency is the same as the running speed of the machine being monitored. For example, if the rotor of an 1800-rpm motor is unbalanced, the rotor will vibrate at 1800 rpm or 30 Hz, and the amount of vibration will be proportional to the amount of unbalance.
Misalignment	Varies	Misalignment of couplings and bearings produces a high axial vibration reading, sometimes up to half as much as the vertical or horizontal vibration readings. This condition generally occurs at the running speed of the machine, although it may also occur at two and three times the running speed.
Looseness	Twice rpm	Mechanical looseness, coupled with misalignment of couplings or bearings, generally causes vibrations that have a frequency of twice the rpm of the machine. Vibration frequency amplitude is usually dependent upon the amount of looseness and the design of the machine.
Resonance	Varies	Each part of a machine, as well as the machine itself, has a resonant frequency. Just as a tuning fork may be "excited" by a shock, small vibration or shock impulses may be synchronized with the resonant frequency of a machine. This synchronization results in a high vibration level at critical machine operating speeds, a level which tapers off above and below each critical speed. Therefore, a machine should not be operated in a resonant condition because the vibration will subject precision parts to undue strain and wear. If a machine must be operated at a speed that falls into the resonant range, the resonant frequency of the machine should be changed—either by raising the frequency by increasing the machine stiffness or by lowering the frequency by increasing the machine mass.
Beat Frequency	Varies	When two frequencies are close to each other, a beat frequency can occur. This beat frequency exhibits itself as a regular rise and fall in amplitude caused by periodic in-phase and out-of-phase conditions of opposing vibrations. Beat frequencies are often found in multiple belt assemblies as a result of slippage in belts. As another example, when motors of nearly identical speeds are mounted on a common base, a small difference in their speeds can cause vibrations to have periodic fluctuations in vibration levels. A beat frequency condition can be eliminated by reducing the level of vibration of one of the sources to the point where it will not materially add or detract from the other source.
Foundation Failure	Unstable	This condition can be determined by erratic changes in vibration amplitude and phase that occur while conducting in-place balancing.

Reprinted with permission. Copyright © by *Automation*.

TABLE 10-14. CHARACTERISTICS OF TYPICAL CAUSES OF MACHINE VIBRATION (Ref. 34)

Vibration Cause	Vibration Frequency (relative to machine rpm)	Characteristics
Bent Shaft	Same or Double	In the case of a bent shaft, a high axial vibration level will occur at the same frequency as machine rpm or in some cases at twice the frequency. For example, if the end of the bent shaft is marked and illuminated with a stroboscope lamp, a single, double, or triple mark will be seen, depending upon the machine design.
Belt Slippage	Varies	Faulty drive belts exhibit an unstable amplitude of vibration and a frequency that ranges from one to five times the rotating speed of the machine. To determine whether a belt is bad, illuminate the belts with a stroboscope lamp. When the stroboscope has been adjusted to "freeze" the belt motion, the relative slippage of one belt among several can be seen.
Gear Noise	Varies	Faulty gears produce a low-amplitude, high-frequency signal, which generally has a definite relationship to the number of gear teeth. In addition to being noisy, the vibration can cause excessive tooth wear or be transmitted to other parts of the machine.
Rolling Element Bearings	20 to 50 Times	In the case of antifriction bearings—such as ball, roller, or needle bearings—scoring or burnelling of the balls or rollers produces a high-frequency, low-amplitude vibration. It is best to use a velocity reading to detect bad bearings of these types since a low-amplitude, high-frequency signal has a high velocity, being a product of frequency and displacement.
Sleeve Bearings	Same	Excessive clearance in sleeve bearings can normally be determined by comparing the vibration measurement on the bearing housing (as close to the shaft as possible) with the vibration level of the shaft itself. If the two measurements are the same, then the vibration is probably being caused by a bad sleeve bearing.
Oil Whip	Lower	This condition may occur in lightly loaded sleeve bearings. Oil whip is indicated by a vibration frequency that is near, but always lower than, the actual shaft speed. Oil whip vibration can be corrected in many cases by one or more ways: (1) changing the lubricant viscosity, (2) changing the bearing or bearing clearances, (3) changing the position of the oil grooves, and/or (4) increasing the bearing load.

automatic systems such as automatic transmissions, which eliminate gear shift levers. Controls also can be designed to facilitate ease of operation in high-vibration environments. An example would be a steering mechanism allowing full travel of the steering wheel without removing the hand. Compound controls enable the operator to adjust several functions without moving his hand from one control to another. The control wheels of many air and ground vehicles contain built-in switches for such functions as changing the radio frequency, controlling a radar or computer, selecting armament, and firing ordnance. This configuration enables the operator to negotiate rough air or rough terrain with precision while performing combat or support functions.

Table 10-13 indicates the characteristics of commonly encountered vibration conditions that designers should attempt to avoid.

10-6.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

The following guidelines are provided to eliminate, reduce, or control the hazards from vibration to personnel and equipment:

1. Whenever possible, use static parts (solid-state parts in electronic equipment).

2. Require that magnetically induced vibration of electrical parts such as transformers be equal to or less than the maximum allowable vibration for the equipment being designed.

3. Design the operator's controls for satisfactory performance of primary and secondary functions in expected vibration environments.

4. Design assemblies of mechanical devices so that alignment of parts is unnecessary. If this is impossible, design for the most advantageous alignment procedure and state alignment requirements in clear, specific terms.

5. Require that all rotating devices be dynamically balanced. State limits of balancing requirements in specifications.

6. Design vibration mounts to

   a. Isolate supporting surface from vibrating equipment

   b. Isolate sensitive equipment from vibrating supporting surfaces.

7. Consider the advantages of rigid mounting of vibrating equipment, and confirm all design solutions to vibration problems through realistic testing requirements.

8. Specify that bearings are to be selected for Army equipment through a 100% test procedure to meet specification requirements. Specify the degree of allowable vibration by thorough consideration of anticipated use, expected environments, and criticality of the equipment to the mission.

9. Where vibration environments exceed the guidance levels indicated in Figs. 10-13 and 10-14, equip the operator's seating with a damped vibration isolation mounting.

10. When an operator must hold vibrating controls for prolonged periods (more than a few minutes at a time), provide the controls with some type of isolation such as foam cushioning to eliminate the vibration.

11. Insure that mass distribution of a mechanical design does not equate to a cantilever beam, which is free to vibrate because of internal or external inputs.

10-7 NOISE

Vibrations within the frequency range of 20 to 20,000 Hz (Ref. 13) are audible to most humans. From our standpoint, the most important portion of that range falls between 300 to 5000 Hz, the frequency range within which most spoken sounds lie. (The ear is most sensitive to sounds in the range from 1000 to 4000 Hz.) Another range of sound, outside the speech range, is also quite necessary

from a military viewpoint. Within this range are the sounds of bells, whistles, and buzzers that warn, alert, and advise.

Noise and blast problems are present in all phases of Army activities. Weapons and other materiel having increased range, velocity, and payload—all releasing greater amounts of acoustical energy that must be controlled—are constantly being produced. These increased noise levels may cause permanent and temporary hearing loss that can affect a soldier's combat efficiency. Increased noise can adversely affect both direct and electrically aided communications between individuals. Such masking effects may result in serious consequences due to misunderstood communications. For certain systems it may be necessary to minimize aural detection by enemy personnel. In this instance, increased noise might produce a system that would be detectable at a distance and that could compromise the performance of the mission of the system (Ref. 13).

Noise information is of importance to the design engineer for two primary reasons, namely,

1. To be aware of the output noise limitations for Army equipment as given in Table 10-2 (Ref. 6), for example

2. To conserve the hearing of personnel and provide for efficient communication between operators by establishing noise levels below certain values based on the category of operator service. Table 10-15 (Ref. 13) gives the sound levels recommended for various applications by the US Army Materiel Command (AMC).

Sounds are generally classified as steady state, produced by various types of rotating or vibrating equipment; or impulse noises, short bursts of acoustic energy consisting of either a single impulse or a series of impulses. The pressure-time history of a single impulse consists of a rapid rise to a peak pressure, followed by a somewhat slower decay to ambient pressure; both rise and fall occur within 1 s (Ref. 6).

The amplitude of sound (noise) at any given point is expressed as the sound-pressure level *SPL*. The physical unit is the decibel (dB) and is expressed as

$$SPL = 20 \log(p/p_o), \text{dB} \qquad (10\text{-}3)$$

where

p = sound pressure being measured, μPa

p_o = reference pressure, usually 20 μPa.

Table 10-16 (Ref. 13) shows the SPL relationship among decibels, pascals, and pounds per square inch. When describing sound, noise, or blast, it is not sufficient to measure the overall SPL because the sensitivity of the human ear to noise is frequency dependent. Thus the noise must be analyzed to determine how the sound energy is distributed over the frequency range. A type of frequency analysis that has gained importance—and

TABLE 10-15. RECOMMENDED SOUND LEVELS FOR VARIOUS APPLICATIONS
(Ref. 13)

Sound Level, dB(A)	Type of Activity	Communication Equivalent	Office Application
108	Maximum design limit for AMC equipment (hearing protection required)	No direct communication is possible.	Not recommended
100	Armored vehicles (hearing protection required)	Electrically aided communication is satisfactory with attenuating helmet or headset; limited shouted communication is possible with difficulty.	Not recommended
90	Materiel that is beyond the state of the art of meeting 85 dB(A) (hearing protection required)	Shouted communication is possible at short distances (0.3-0.6 m) (1-2 ft).	Not recommended
85	Acceptable level for unprotected hearing for 8-h exposures	Shouted communication is possible at several feet (0.9-1.2 m) (3-4 ft). Telephone use is difficult.	Not recommended
75	Maintenance shops, garages, keypunch areas	Occasional telephone use and occasional direct communication at up to 1.5 m (5 ft) is acceptable.	Not recommended
65	Operation centers, mobile command and communication centers, computer rooms, word processing centers, kitchens, laundries	Frequent telephone use and frequent direct communication at up to 1.5 m (5 ft) are acceptable.	Business machine offices
55	Drafting rooms, laboratories, conferences with 2 or 3 people	No difficulty with telephone use, and occasional direct communication at up to 4.5 m (15 ft) is possible.	Shop offices, general secretarial areas
45	Libraries, conference rooms, command and control centers, theaters, sleeping areas	No difficulty with direct communication exists.	General offices

which has been adopted by the Army—is the "weighting network" included in all sound-level meters that meet the current requirements of the American National Standards Institute's (ANSI) specification for sound-level meters. For example, if an A-weighted SPL of 80 is obtained, the value would be reported as 80 dB(A). The A-weighting network is particularly valuable in estimating the interference of noise upon speech. Fig. 10-16 (Ref. 13) illustrates the frequency dependence of the human ear relative to a hearing hazard, e.g., for an A-weighted sound level of 90 dB(A), the SPLs of 85 dB at 2000 Hz and 95 dB at 200 Hz are interpreted by the ear as providing an

equivalent hazard. The Army limits the noise environment to 85 dB(A) for an 8-h-day exposure unless the operator is provided with a noise-attenuating device. Table 10-17 (Ref. 13) indicates time-exposure values for various noise levels for continuous noise environments. Note from Table 10-17 that for each decrease of 4 dB(A), the allowable exposure time is doubled. Table 10-18 (Ref. 35) lists the sound pressure levels of common noises and their effects on personnel. Table 10-19 (Ref. 13) lists peak pressure levels at crew locations for representative Army weapons.

TABLE 10-16. RELATIONSHIP AMONG DECIBELS, PASCALS, AND POUNDS PER SQUARE INCH (Ref. 13)

dB*	Pa	psi
0	0.00002	2.90×10^{-9}
14	0.0001	14.50×10^{-9}
34	0.001	145.00×10^{-9}
54	0.01	1.45×10^{-6}
74	0.1	14.50×10^{-6}
94	1	145.00×10^{-6}
114	10	1.45×10^{-3}
134	100	14.50×10^{-3}
154	1000	145.00×10^{-3}
174	10,000	1.45×10^{0}

*These values derive directly from the application of Eq. 10-3. For example, determine the decibels corresponding to an $SPL = 1$ Pa.

$$dB = 20 \log (1/0.00002) = 20 \log 50,000$$
$$= 20(4.70) = 94.$$
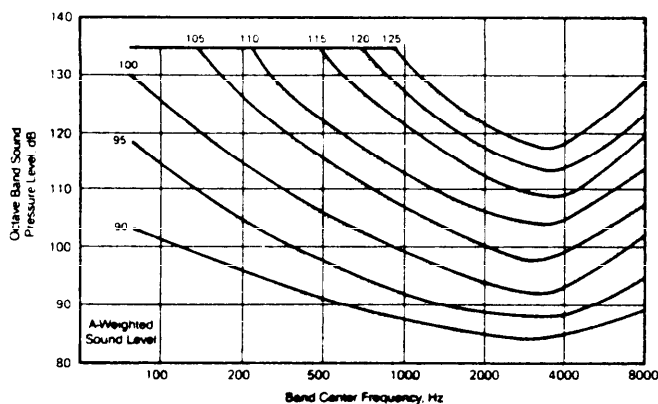
Figure 10-16. Contours for Determining Equivalent A-Weighted Sound Level (Ref. 13)

TABLE 10-17. LIMITING EXPOSURE TIMES FOR VARIOUS VALUES OF NOISE LEVELS (Ref. 13)*

Exposure Time, min	Maximum Noise Level, dB(A)
960	81
480	85
240	89
120	93
60	97
30	101
15	105
7.5	109
3.75	113

*When the exposure is intermittent at different sound levels, the fraction

$$A_1/T_1 + A_2/T_2 + \cdots + A_n/T_n$$

where
A_i = total exposure time at the specific noise level, min, $i = 1,2,...,n$
T_i = limiting exposure time for a particular noise level, min, $i = 1,2,...,n$

should not exceed unity to meet the exposure limitation.

TABLE 10-18. COMMON NOISES (Ref. 35)

Sound Pressure, Pa	Sound Pressure Level, dB	Source or Effect of Noise
200	140	Threshold of pain
	130	Pneumatic rock drill
20	120	Loud automobile horn
	110	Punch press
0.2	100	Automatic lathe
	90	Noisy factory
0.2	80	Passing truck
	70	Noisy office
0.02	60	Conversational speech
	50	Business office
0.002	40	Average residence
	30	Broadcast studio
0.0002	20	Rustle of leaves
	15	Average threshold
0.00002	0	Acute threshold

TABLE 10-19. PEAK PRESSURE LEVELS AT CREW STATIONS FOR VARIOUS ARMY WEAPONS (Ref. 13)

Weapon System	Peak Pressure Level, dB
Rifle, M16	154
REDEYE	157
STINGER	165
90-mm Recoilless Rifle	181
105-mm Howitzer	177

The military services have established 140 dB as the maximum impulsive sound level that personnel may be exposed to without hearing protection. Table 10-20 (Ref. 6) and the supporting Fig. 10-17 (Ref. 6) provide guidance for designers faced with impulse noise problems. Note that—regardless of the type of protection indicated in Table 10-20—peak pressure levels for impulse noise should not exceed approximately 189 dB even for 1 ms and should not exceed approximately 176 dB beyond 200-ms duration. Observe that the W line at 140 dB is far below either the X, Y, or Z lines. In the application of Table 10-17, a single exposure consists of either (1) a single pulse of sound from a nonrepetitive system—systems producing not more than one impulse per

TABLE 10-20. IMPULSE NOISE LIMIT SELECTION CRITERIA (Ref. 6)

Maximum Expected Number of Exposures in a Single Day	Impulse Noise Limit		
	No Protection	Either Plugs or Muffs	Both Plugs and Muffs
1000	W	X	Y
100	W	Y	Z
5	W	Z	Z
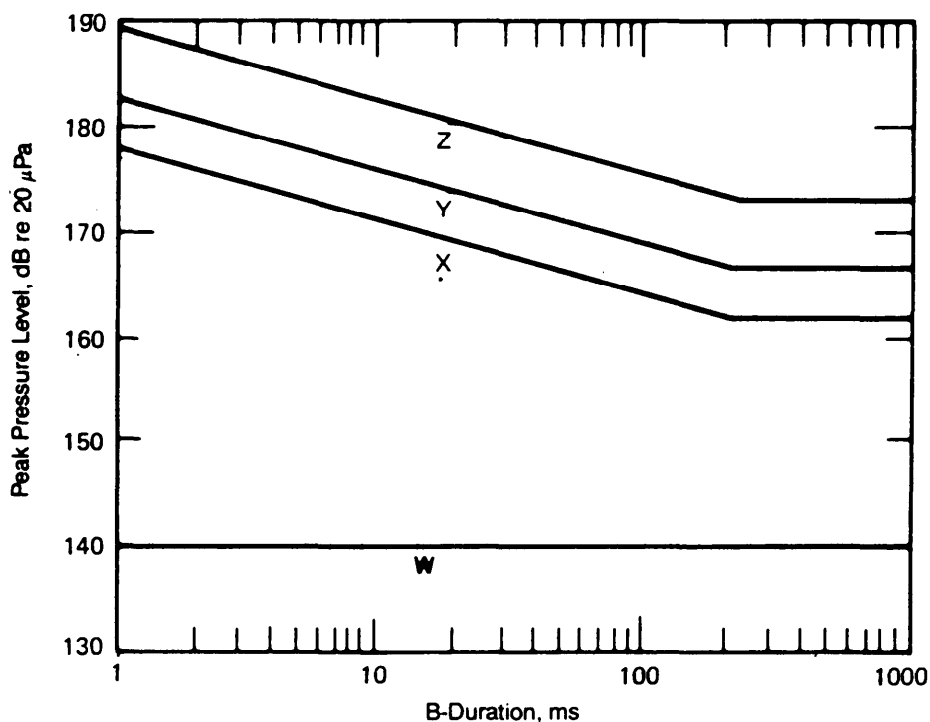
B-Duration (Pressure Envelope Duration) is "The duration of the primary portion of an impulse noise plus the duration of significant subsequent fluctuations. These durations are considered to be the time interval during which the envelope of pressure fluctuations (positive and negative) is within 20 dB of the peak pressure level. Significant subsequent pressure fluctuations are those whose summed duration is greater than 10% of the duration of the primary portion. The primary portion of an impulse noise is that period of time which is followed by a level which remains 20 dB below the peak pressure level for a significant duration." (Ref. 6). The method for determining B-duration is described in Ref. 6.

Figure 10-17. Peak Pressure Level and B-Duration Limits for Impulse Noise (Ref. 6)

second—e.g., semiautomatic weapons or (2) a burst of sound impulses from a repetitive system—systems normally producing more than one impulse per second—e.g., automatic weapons. Higher pressure levels than the Z line are not permitted due to the possibility of other non-auditory physiological injury. Hearing loss generally occurs first in the vicinity of 4000 Hz—a very serious effect because this is the range of speech at which consonants are usually sounded.

Shock waves generated by explosions can produce high sound pressures that can rupture the eardrum. Normally, the shock wave with elevated pressure occurs only once; it is not vibratory in nature as is the general case with noise. Very loud noises (above the Z line of Fig. 10-17) may cause a ringing in the ears and temporary deafness; they may also cause nonauditory physiological injury. Another adverse effect of these loud noises is that they trigger the startle reflex mechanism in the body, which releases adrenalin into the bloodstream and causes a tightening of the blood vessels to prepare the body for "fight or flight". The danger is that a person may be startled into taking an undesired action—such as inadvertently activating a piece of equipment, falling off an elevated surface, or jumping into the path of a moving vehicle—that will cause an accident. Repeated reactions to sudden loud noises will also cause fatigue.

Continuous noises, whether loud or soft, can be distracting; they may interfere with normal communica-tion or simply irritate the hearer. The sound of voices just below the comprehension level can be especially dis-tracting as can two oral messages arriving simultaneously. Personnel who operate machinery or perform other high-concentration tasks are susceptible to errors if noise distracts them.

10-7.1 TOLERANCE AND SAFE EXPOSURE LIMITS

The safe exposure limit stipulated by OSHA standards is 90 dB for an 8-h exposure to steady state noise. It has been found that hearing loss from long exposure will occur at levels above 85 dB(A); accordingly, the National Institute of Occupational Safety and Health (NIOSH) has recommended that the OSHA standard be revised to this level. For that reason, the Army uses the 85-dB(A) limit in MIL-STD-1474 (Ref. 6).

Military specifications and standards contain require-ments for safe exposure limits in addition to the require-ments that all OSHA standards be met, but requirements for noise control to prevent communications interference are generally more strict. Table 10-21 (Ref. 6) lists noise limit categories as a function of system requirements for steady state noise. The corresponding upper noise limits are shown in Table 10-22 (Ref. 6).

In reference to Table 10-22, for those cases in which the mission profile for the equipment being developed exceeds 8 h of operation in each 24-h period, the limits specified in

TABLE 10-21. STEADY STATE NOISE CATEGORIES (Ref. 6)

System Requirement	Category
No direct person-to-person voice communication required. *Maximum design limit.* Hearing protec-tion required.	A
System requirement for electrically aided communication via attenuating helmet or headset. Noise levels are hazardous to unprotected ears.	B
No frequent direct person-to-person voice communication required. Occasional shouted communi-cation may be possible at a distance of 0.3 m (1 ft). Hearing protection required.	C
No frequent direct person-to-person voice communication required. Occasional shouted communi-cation may be possible at a distance of 0.6 m (2 ft). Levels in excess of Category D require hearing protection.	D
Occasional telephone or radio use or occasional communication at distances up to 1.5 m (5 ft) required. (Equivalent to NC-70.)+	E*
Frequent telephone or radio use or frequent direct communication at distances up to 1.5 m (5 ft) required. (Equivalent to NC-60.)+	F*

+NC = noise criterion curves
*For design of mobile or transportable systems. For fixed-plant facilities, see MIL-STD-1472.
Categories A, B, C, and D are based primarily on hearing conservation priorities; E and F are based primarily on communication priorities.

TABLE 10-22. STEADY STATE NOISE LIMITS FOR CATEGORIES OF PERSONNEL-OCCUPIED AREAS (Ref. 6)

Octave Band Center Frequency	Category					
	A	B	C	D	E	F
63 Hz	130 dB	121 dB	111 dB	106 dB		
125	119	111	101	96		
250	110	103	94	89		
500	106	102	88	83		
1000	105	100	85	80		
2000	112	100	84	79		
4000	110	100	84	79		
8000	110	100	86	81		
dB (A) Criteria	108	100	90	<85	75	65
Alternate PSIL-4 Criteria					67	57

Categories A-D shall be reduced sufficiently to allow for an exposure for longer than 8 h, as approved by the acquisition activity in conjunction with the Surgeon General's Office, HDQA, DASG-PSP, Washington, DC 20314. The criteria in Categories E and F are defined by either the sound level, in dB(A), or the preferred speech interference level (PSIL-4). The dB(A) sound level is the desired requirement. Where it is not possible to meet the specified dB(A) level, the corresponding PSIL-4 requirements shall be met.

Many military standards, regulations, and technical bulletins provide guidance for designers in acoustic noise generation limits and protection to personnel. MIL-STD-1474 (Ref. 6) has been referenced several times, and pertinent tables and figures from that standard are included in this handbook. In general, the data in that standard are taken from or guided by the information in AR 40-5 (Ref. 36), TB MED 501 (Ref. 37), and various reports from the National Institute of Health and Safety.

Designers may be required to keep the noise generated by their equipment within certain nondetectability limits. Guidance for aural nondetectability is provided in Table 10-23 (Ref. 6). The following quotation is taken from Ref. 6:

"Unless otherwise specified by the procuring activity, the octave band pressure level limits shown in... [Table 10-23] shall not be exceeded by those items of equipment having an aural nondetectability requirement. These limits are for nondetectability under commonly found favorable sound propagation conditions. The actual detection distance for specific conditions of terrain, wind, background noise, etc., may occasionally be greater but more often will be smaller. The octave band pressure levels at the 'measurement distances' must not be exceeded

in any band if nondetectability is to be achieved at the corresponding 'nominal nondetectability distances'.".

Tolerance of noise is a human characteristic different from noise-damage hearing conservation limits; tolerances vary widely, depending on the sensitivities, likes and dislikes, age, and occupation of the individuals concerned. Not only must designers observe the communications levels for military equipment in which accurate communication is critical to the success of the mission, but they must also consider the sensitivity of the operators' concentration requirement and the effects upon concentration of various types of noise. Harsh or "screechy" sounds that might be irritating to the average person—and particularly to one concentrating on his task—should be avoided.

10-7.2 POTENTIAL HAZARD SOURCES

Since noise is generally the result of vibration, the causes of sound-generating vibration will be the same as those indicated in par. 10-6.2 on causes of mechanical vibration. In addition, impulsive noises can be generated by explosions such as gunfire, missile launchings, and ruptures of pressure vessels that produce shock waves. A slight imbalance in rotating devices, electric brush friction and bounce, loose magnetic lamination materials, and vibrations in air ducts can produce noise of different frequencies and human irritation characteristics. The mountings of dynamic equipment can also contribute to the subsystem noise.

In some instances the noise-generation characteristics of developmental equipment may not be known until prototypes have been built and tested. Prototype testing to locate noise generators is an effective way to determine the need for additional noise control. This type of testing

TABLE 10-23. LIMITING OCTAVE BAND LEVELS (dB)
FOR AURAL NONDETECTABILITY (Ref. 6)

Measurement Distance,		Center Frequency, Hz								Nominal Non-detectability Distance,	
m	ft	63	125	250	500	1k	2k	4k	8k	m	ft
1.25	4.1	48	34	32	32	32	32	32	32	5	16.4
2	6.6	50	36	34	34	34	34	34	34	10	32.8
2	6.6	56	42	40	40	40	40	40	41	20	65.6
2	6.6	60	46	44	44	44	44	44	45	30	98.0
6	19.7	60	46	44	45	45	45	47	48	100	328.0
10	32.8	62	48	46	46	47	48	51	53	200	656.2
10	32.8	66	52	50	50	51	53	57	61	300	984.3
15	49.2	65	51	49	49	50	53	58	64	400	1312.3
20	65.6	64	50	48	49	50	53	60	67	500	1640.4
25	82.0	66	52	50	51	53	58	68	78	750	2460.6
25	82.0	68	54	52	54	57	63	77	90	1000	3280.8
50	164.0	62	48	46	48	51	56	70	83	1000	3280.8
25	82.0	70	56	54	56	60	67	85	102	1250	4101.0
25	82.0	72	58	56	59	63	72	93	113	1500	4921.3
25	82.0	74	60	58	62	68	80	108	135	2000	6561.7
50	164.0	68	54	52	56	62	73	102	128	2000	6561.7
50	164.0	72	58	56	61	70	88	131	N/A	3000	9482.5
25	82.0	80	66	64	72	84	108	N/A	N/A	4000	13,123.4
50	164.0	74	60	58	66	78	102	N/A	N/A	4000	13,123.4
50	164.0	76	62	60	70	85	114	N/A	N/A	5000	16,404.2
50	164.0	78	64	62	73	91	127	N/A	N/A	6000	19,685.0

is always required for vehicles, construction and material handling equipment, mobile generator sets, and air compressors—all of which can develop noise in unpredictable ways. This unpredictable aspect of the noise problem is due to the complexity of the various arrangements of moving parts, structures that could transmit vibrations, natural frequencies of parts joined into an assembly, and other factors. Ref. 38 indicates the ways tracked vehicles were tested to evaluate sources of noise so that corrective measures could be developed. MIL-STD-1474 (Ref. 6) should be consulted for test requirements, procedures, and data to be recorded for each separate element of the noise control design problem.

10-7.3 HAZARD CONTROL TECHNIQUES*

Designing to eliminate noise must begin with a careful analysis of the potential sources of noise. Whenever a design contains dynamic components such as gases or liquids in motion, or electrical parts subjected to various electrical frequencies, the analyst should look for the possible sources of noise generation. Even nondynamic electronic components of radar equipment can generate significant noise. Remedies include

1. Changing the mass or mass distribution of

*An excellent article on the technical background of noise and its control can be found in Ref. 39.

magnetic materials in the microwave components and high-voltage power supplies

2. Increasing the uniform tightness and physical security of magnetic material laminations and at all other surfaces of mating parts wherever they occur in the design

3. Insuring the balance of all rotating equipment

4. Controlling the number and relative locations of cooling blades and openings in rotating equipment to eliminate the "siren" effect

5. Selecting a brush material that reduces generated acoustic noise

6. Mounting dynamic components in a manner that reduces transmitted vibration

7. Eliminating air flow path sources of "audio reeds" that will generate noise.

Even jet engine noise, a hazard to personnel in the vicinity of Army helicopters and some light aircraft, can be reduced by design. The inlet and exhaust lining designs of jet engines can be detailed to provide many tiny "acoustic traps" and noise-cancelling openings, which greatly decrease the noise level.

Design techniques for control of noise hazards can be divided into (1) elimination or control of sound (already discussed) and (2) protection of personnel from the sound. If noise cannot be eliminated at its sources, then personnel must be protected. Personnel protection falls

into two broad categories: (1) isolation and separation and (2) individual protective devices. Each category is discussed in the subparagraphs that follow. Neither AR 40-5 (Ref. 36) nor OSHA regulations consider personal protective devices suitable substitutes for noise abatement, although such devices may be required when noise cannot be controlled to an adequately low level.

Isolation and separation techniques include

    1. Use of soundproof enclosure to separate personnel from noise or vice versa

    2. Use of sound-absorbing walls and baffles between personnel and high-noise environments

    3. Assurance that walls, floors, and partitions do not transmit noises by isolating them from the vibrating source in the design

    4. Assurance that ducting and piping do not transmit noise through soundproof enclosures.

Individual protective devices are plugs worn in the ears or muffs worn over the ears as shown in Fig. 10-18 (Ref. 40). Earplugs are made from rubber or plastic and are available in a variety of sizes. Some of the types of newer plastic plugs are readily malleable and will easily conform to the individual ear, but some people suffer discomfort from plugs. The most efficient types of earplugs will protect the wearer from an 8-h exposure to 95-dB noise levels. Waxed cotton and "swedish wool" protectors made of very fine glass fibers are almost as effective as plugs. They are malleable and conform to the ear and, therefore, are more comfortable than plugs. They are designed to be used once and thrown away, a feature that makes them more sanitary but more expensive. The
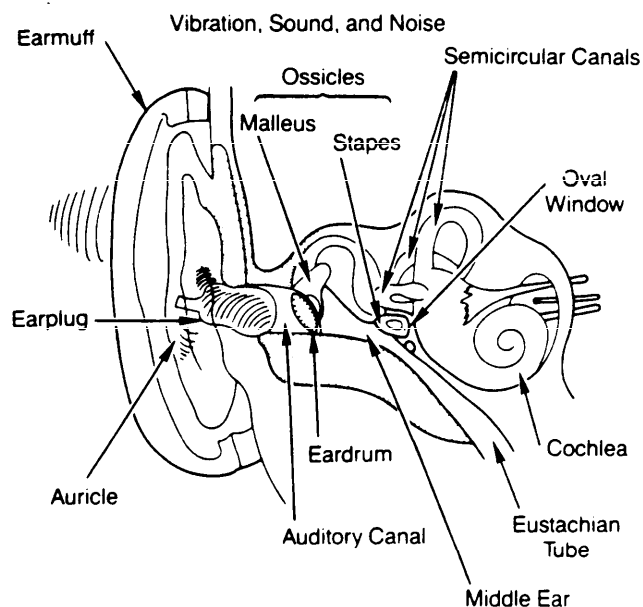
Reprinted with permission. Copyright © by *Sound and Vibration.*

Figure 10-18.   Individual Protective Devices—Earplugs and Earmuffs (Ref. 40)

disadvantage to both plugs and wools is that a supervisor cannot readily see whether a person is wearing them. An additional disadvantage is that they do not protect against transmission of sound through the bone structure surrounding the ear.

Earmuffs cover the entire ear and the surrounding area; therefore, they provide greater protection than plugs and wools. They are individually adjustable and can be removed easily. The pressure against the side of the head creates discomfort to some people, especially to the wearers of glasses with temples of round cross-section. Earmuffs also are uncomfortable in high-temperature environments that cause profuse perspiration. Fig. 10-19 (Ref. 41) illustrates several types of ear protectors.

10-7.4   SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

The following guidelines should be applied to eliminate, reduce, or control the noise hazard to personnel:

    1. Review the concept for the design and determine the most likely sources of acoustic noise.

    2. Based on field data of similar equipment, deter-
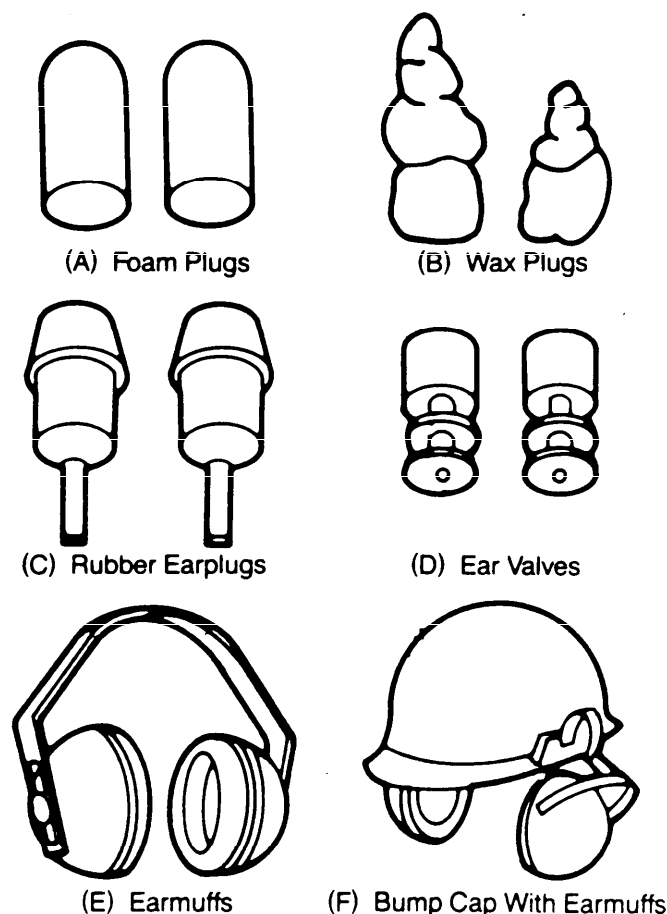
Reprinted with permission. Copyright © by Industrial Indemnity Company.

Figure 10-19. Types of Ear Protectors (Ref. 41)

mine the ranges of sound level and frequency probable in the present design.

3. Consult tables of allowable sound levels in MIL-STD-1474. (The tables in this handbook are from MIL-STD-1474B (Ref. 6); however, the latest issue should be reviewed for possible changes.)

4. Provide design features, including specification of the allowable unbalance in rotating equipment, that will keep the generation of vibratory sound within acceptable limits.

5. When it is anticipated that noise will unavoidably exceed the allowable levels, design acoustic enclosures, separators, and mountings to control the noise that will reach operators.

6. Use lead, other soft materials, and known sound-absorbing designs for walls and baffles where these materials can be used without creating serious design problems.

7. Where performance requirements or military necessity rule out any possibility of meeting acceptable sound levels, specify hearing protectors for operators.

8. During testing to establish the sound levels of the design, use caution signs as shown in Fig. 10-20 (Ref. 6). Design these signs to be placed on equipment that will not meet the requirements for unprotected hearing levels.

10-8 RADIATION

Radiation is a form of energy whose presence, with minor exceptions, cannot be seen, felt, smelled, heard, or tasted. Electromagnetic radiation is classified into a number of types, depending on the frequency at which it occurs. Generally, the higher the frequency—and the shorter the wavelength—of the electromagnetic radiation, the more severe the hazard and the injuries that can be caused for a given exposure time.

Radiation in general is divided into two categories, i.e., ionizing and nonionizing. Both ionizing and nonionizing radiation can cause injury. Ionizing radiations are X rays,

Black ← Yellow →

HIGH INTENSITY NOISE

HEARING PROTECTION REQUIRED

Note: Sizes should be proportional in accordance with MIL-STD-1473 and should be sufficiently large to insure legibility at required reading distances.

Figure 10-20. Noise Hazard Caution Sign (Ref. 6)

gamma rays, alpha and beta particles, neutrons, and other nuclear particles. High-frequency ionizing radiation produces harmful effects in biological systems by altering the functioning of cells. Nonionizing radiation does not have energy sufficient to "ionize" tissues but has other adverse effects such as disorders of the central nervous system, eye and tissue burns, and temporary blindness. Ultraviolet, infrared, visible optical radiation, and microwave radiation are examples of nonionizing radiations.

Nonionizing radiation, with its lower energies, lies in the lower and central regions of the electromagnetic spectrum. This portion of the spectrum ranges from radio waves and microwaves at the lower frequencies (longer wavelengths), through the optical radiation—infrared, visible light, and ultraviolet—at the higher frequencies. Ionizing radiation begins at the far ultraviolet (ultra high frequencies) and extends to soft X rays, hard X rays, and gamma rays located in the upper part of the electromagnetic spectrum. A portion of the electromagnetic spectrum showing these areas is shown in Fig. 10-21. Radio frequency bands, from very low frequency (VLF) to extremely high frequency (EHF), are shown under hertzian waves.

To avoid possible confusion as to the units by which radiation and its effects on the human body are measured—roentgen (R), radiation absorbed dose (rad), relative biological effectiveness (rbe), and roentgen-equivalent man (rem)—a brief discussion follows:

1. *Roentgen.* The roentgen measures an exposure dose of gamma radiation or X rays. Since the interaction of gamma radiation and X rays with matter results in the production of ion pairs, an R is defined as the quantity of gamma radiation or X rays that will give rise to the formation of 2.08×10^9 ion pairs per cubic centimeter of dry air at a standard temperature of $0°C$ and a standard pressure of 1 atm. This is equivalent to the release of about 83 ergs of energy when 1 g of dry air under standard conditions is exposed to 1 R of gamma radiation. Since the roentgen refers to a specific result in air accompanying the amount of radiation through air, it does not imply any effect it would produce in a biological system. The effect on a biological system is expressed in terms of an absorbed dose described in the paragraph that follows.

2. *Radiation Absorbed Dose (rad).* The rad measures exposure dose and is defined as the absorbed dose of any nuclear radiation that is accompanied by the release of 10^{-5} joules of energy per gram (100 erg/g) of absorbing material, i.e., the release of 100 ergs/g in any absorbing medium.

3. *Relative Biological Effectiveness (rbe).* Although all ionizing radiations are capable of producing similar biological effects, the absorbed dose in rads that will produce a certain effect may vary appreciably from one type of radiation to another. This difference in behavior is expressed by means of the rbe of the particular nuclear
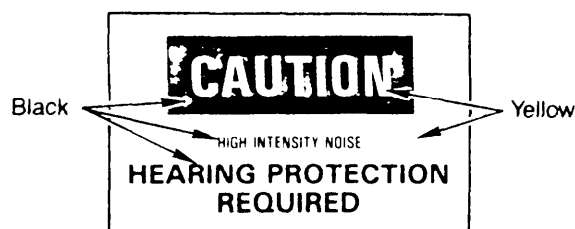
Photon Energy, eV

10^{-10} 10^{-9} 10^{-8} 10^{-7} 10^{-6} 10^{-5} 10^{-4} 10^{-3} 10^{-2} 0.1 1 10 10^2 10^3 10^4 10^5

	Radar		Infrared Rays		Visible Light		X Rays →
Microwaves						Ultraviolet Rays
Hertzian Waves				

| VLF | LF | MF | HF | VHF | UHF | SHF | EHF |

0.03　0.3　3　30　300　3×10^3　3×10^4　3×10^5　3×10^6　3×10^7　3×10^8　3×10^9　3×10^{10}　3×10^{11}　3×10^{12}

Frequency, MHz

10^6 10^5 10^4 10^3 10^2 10 1 0.1 10^{-2} 10^{-3} 10^{-4} 10^{-5} 10^{-6} 10^{-7} 10^{-8}

Wavelength, cm
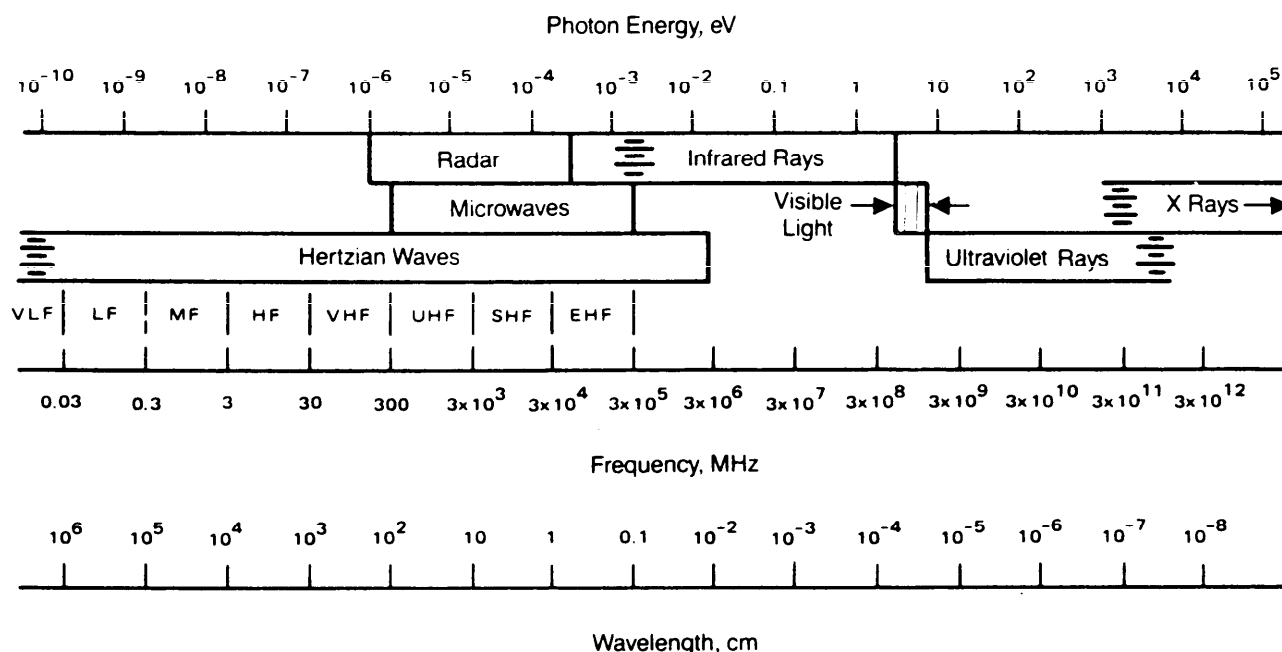
Figure 10-21. Electromagnetic Spectrum

radiation. Thus the rbe of a given radiation is defined as the ratio of the absorbed dose in rads of gamma radiation to the absorbed dose in rads of the given radiation having the same biological effect. The rbe value for a particular type of nuclear radiation depends on the dose rate, the energy of the radiation, the kind and degree of the biological damage, and the nature of the tissue under consideration. Fig. 10-22 (Ref. 15) lists rbe values for various types of nuclear radiations.

4. *Roentgen-Equivalent Man (rem)*. The rem is a dose unit of biological effect. The rad is a convenient unit, for expressing energy absorption, but it does not take into account the rbe of the particular type of nuclear radiation absorbed. The rem, however, which is defined as

$$\text{Dose in rems} = (\text{rbe}) \times (\text{dose in rads}) \quad (10\text{-}4)$$

provides an indication of the extent of the biological injury that would result from the absorption of nuclear radiation. Fig. 10-22 (Ref. 15) illustrates the relationship among rad, rbe, and rem.

10-8.1 IONIZING RADIATION

Nuclear particles (alpha, beta, and neutrons), X rays, and gamma rays are ionizing radiations. Neutrons, gamma rays, and X rays—since they have no charge—produce ionization indirectly. These radiations cause injury by ionizing or exciting cellular components of the biological system, which results in functional changes. The susceptibility of tissues to damage varies and depends upon their composition, form, and function. Various organs and tissues exhibit specific sensitivities and thus

respond differently to ionizing radiations. Some damage can be repaired by natural processes within the cell and is reversible damage; otherwise, the damage is irreversible. Ref. 42 presents a detailed discussion of the biological effects of nuclear radiation on the human body.

Neutrons, being electrically neutral particles, do not produce ionization or excitation directly in their passage through matter. They can, however, cause ionization to occur indirectly as a result of their interaction with certain light nuclei, e.g., collision with the nucleus of a hydrogen atom. Fast neutrons are also captured by nitrogen nuclei with the subsequent emission of protons capable of producing ionization. Being neutral, the neutron can penetrate matter and, therefore, makes shielding more difficult.

Regardless of the type of ionizing radiation, the end result is injury to the biological system and, in extreme cases, death. The factors that determine the extent of the injury are the type of radiation, total dose, rate of absorption, and region and extent of the body exposed.

The damage resulting from exposure to ionizing radiation is not limited to living tissue; materials also are affected. The magnitude of the damage resulting from nuclear radiation is a function of the amount of energy deposited within the material and the form that the energy deposition assumes. Thus if a material absorbs little radiation, it may be unaffected in many applications. If the energy deposition is large, a material may lose its intended properties—elastomers lose their flexibility, metals and concrete experience reduced physical properties, plastics lose their transparency, and lubricating and hydraulic oils change their properties. Solid-state

Roentgen	RAD		REM
83 ergs/gram dry air, Used in measuring exposure dose from x- and gamma radiation only.	100 ergs/gram any medium	× RBE	Applied to man, and corrects for specific ionization effects of the radiation.
	*R*adiation *A*bsorbed *D*ose	*R*elative *B*iological *E*ffectiveness	*R*oentgen *E*quivalent *M*an

Type of Radiation	RBE
X rays	1
Gamma rays	1
Beta particles, 1.0 MeV	1
0.1 MeV	1
Neutrons, thermal energy	2.8
0.0001 MeV	2.2
0.005 MeV	2.4
0.02 MeV	5
0.5 MeV	10.2
1.0 MeV	10.5
10.0 MeV	6.4
Protons, greater than 100 MeV	1-2
1.0 MeV	8.5
0.1 MeV	10
Alpha particles, 5 MeV	15
1 MeV	20

Figure 10-22. Radiation Terms and RBE Values (Ref. 15)

electronic devices (integrated circuits) are extremely sensitive to nuclear radiation because their operation is very sensitive to the structure of the material. Absorbed radiation that ionizes an atom or displaces an atom in a semiconductor or microchip will affect the operation of the device that uses the material.

10-8.1.1 X Rays and Gamma Rays

Gamma radiation—emitted by radioactive materials both man-made or natural—and X rays (because of their high energies) have the ability to penetrate dense materials. It is this characteristic that allows the radiation to penetrate the body and produce tissue damage as well as skin damage.

X rays are a common source of ionizing radiation and

result whenever high-speed electrons strike a metal target. For the electrons to be accelerated to this speed, a potential difference of 12,000 to 15,000 V generally is required. Where voltages exceed 15,000 V, the possibility of an X-ray hazard is substantial. Therefore, designers can avoid X-ray hazards by keeping voltages below 10,000 V or using nonmetallic targets whenever feasible. To be on the safe side, any electrical equipment operating at or above a potential difference of 10,000 V should be surveyed periodically with a radiation detector, e.g., a Geiger counter.

Gamma radiation is emitted by radioactive materials in the natural decay process. Therefore, to avoid a gamma radiation hazard, use of radioactive materials must be avoided wherever possible. If an emitter material is used,

TABLE 10-24. RADIATION EXPOSURE LIMITATIONS (Refs. 41 & 44)

Maximum Permissible Dose Equivalent For Occupational Exposure	
Combined & Whole-Body Occupational Exposure	
Prospective Annual Limit	5 rems in any one year
Consecutive Weeks	3 rems in 13 weeks
Retrospective Annual Limit	10-15 rems in any one year
Long-Term Accumulation to Age N Years	$(N-18) \times 5$ rems
Skin	15 rems in any one year
Hands	75 rems in any one year (25/quarter)
Forearms	30 rems in any one year (10/quarter)
Other Organs, Tissues, and Organ Systems	15 rems in any one year (5/quarter)
Fertile Women (with respect to fetus)	0.5 rem in gestation period

Nonoccupational exposures, including students and minors, are limited to 10% of the maximum permissible dose equivalent for occupational exposures.

Reprinted with permission. Copyright © by Industrial Indemnity Company.

proper shielding must be employed to reduce the radiation to a safe level. Ref. 43 contains a complete listing of radioactive isotopes, their method of decay, particle or gamma ray energy, and half life. Table 10-24 (Refs. 41 and 44) gives radiation exposure limits for (1) combined and whole-body occupational exposure and (2) nonoccupational exposures including students and minors.

10-8.1.2 Alpha and Beta Particles

Alpha particles, identical with the nucleus of a helium atom, are emitted in radioactive decay. Because of their mass—approximately 7300 times that of an electron—and their charge, alpha particles do not possess much penetrating power. In its passage through matter, the alpha particle produces considerable direct ionization and thereby loses energy rapidly. Consequently, an alpha particle will traverse only a few centimeters of air before coming to rest. Normally, alpha particles will not penetrate the skin. However, if alpha emitters enter the body in sufficient quantity by ingestion, inhalation, or through skin abrasions, the effects may become serious.

Thorium, which is used in optical coatings, in magnesium alloys for strength, and in thoriated tungsten welding rods, is an example of an alpha emitter with wide application in industry and in Army equipment. It is most hazardous in the form of dust or fumes generated when its alloys are machined, ground, or welded. Consequently, precautions must be taken to avoid inhaling or ingesting thorium particles. Masks, ventilation hoods, respirators, protective clothing, gloves, and other protective measures to prevent contamination should be used when handling alpha or beta particle emitters.

Beta particles usually, but not always, are emitted with gamma radiation in nuclear decay. The beta particle, identical to an electron, travels at a high speed, which depends upon its source. Beta particles, like alpha

particles, are able to cause direct ionization in their passage through matter. The beta particles dissipate their energy less rapidly than alpha particles and, consequently, have a greater range in air and other materials. An energetic beta particle can penetrate the outer layer of the skin; however, the main hazard associated with beta particles arises from materials ingested or inhaled or from direct contact with the skin. The potential hazard for beta skin burns was evidenced by the injuries received by the Marshall islanders in March 1954 when they were accidently subjected to fallout from a nuclear detonation at the Pacific Proving Ground (Ref. 45).

Any radioactive materials entering the body through the ingestion of contaminated food, breathing of contaminated air, or through wounds or abrasions can produce considerable injury to the biological system. The exposure is continuous and is subject only to depletion of the quantity of active material in the body as a result of physical (radioactive decay) and biological (elimination) processes. The harmful effects of these internal radiation sources are compounded by the fact that certain compounds or elements localize in specific tissues, which are then subjected to a concentrated radiation source (Ref. 46).

10-8.1.3 Shielding

Alpha particles can be shielded against more easily than beta particles. Thin paper will stop most alpha particles. A thin metal foil will stop most beta particles; clothing will also offer considerable protection. It is important to choose the metal foil carefully, however, in order to minimize the possibility that X rays will be generated as a result of an energetic beta particle striking a metal target. When shielding high-energy beta sources, lighter, less dense shielding materials, e.g., aluminum or lucite, will produce fewer X rays than lead or iron. Table

TABLE 10-25. SHIELDING RECOMMENDATIONS FOR PROTECTION FROM IONIZING RADIATION (Adapted from Ref. 46)

Radiation Type	Range in Air	Shield Material	
		Type	Thickness, mm (in.)
Thickness of Materials That Will Stop Alpha & Beta Particles			
Alpha (4 MeV)	28 mm (1.102 in.)	Aluminum Sheet	0.396 (0.0156)
		Paper	0.396 (0.0156)
		Ordinary Clothing	0.396 (0.0156)
Beta (3 MeV)	13.0 m (42.65 ft)	Lead	1.4 (0.055)
		Aluminum	5.3 (0.209)
		Pyrex	6.6 (0.26)
		Lucite	12.4 (0.488)
		Water	14.8 (0.583)
Half-Value Thickness of Materials That Will Reduce Gamma Radiation			
Gamma (4 MeV)	Long Range (several miles)	Lead	7.6 (0.3)
		Iron	12.7 (0.5)
		Aluminum	68.58 (2.7)
		Concrete	68.58 (2.7)
		Water	210.8 (8.3)

Information for this table is from R. E. Barbiere, *et al.*, *A Radiobiology Guide*, Wright Aeronautical Development Center Technical Report 57-118, Wright Aeronautical Development Center, Wright-Patterson AFB, OH, 1958.

10-25 (Ref. 46) indicates various thicknesses of materials that will stop alpha and beta particles.

In theory, gamma and X radiations can never be totally eliminated by shielding, but they can be attenuated to a safe operating level. Heavy metals such as iron and lead make good shields because of their high density—the higher the density, the better the shield. Table 10-25 (Ref. 46) indicates the half-thickness values of various materials for attenuating 4 MeV gamma rays, i.e., the thickness of the specified material that will reduce the radiation dose (or dose rate) by one half. A more energetic gamma ray would require an increased thickness. The half-thickness values in Table 10-25 also can be used for attenuating hard X rays; however, the indicated values are conservative. Designers faced with structural or facility radiation protection problems can find guidance in the publications of the National Council on Radiation Protection (NCRP), P. O. Box 30175, Washington, DC 20014. Because of gamma ray scattering, a shield situated to block the source of the radiation will provide only partial protection from injury. For effective protection, the shielding must provide protection in all directions.

Neutrons, because of their neutral charge and high energy—some neutrons from a nuclear reactor travel with an energy of 10 MeV—are difficult to attenuate and are capable of penetrating various materials, including the human body, to great depths. A complication in neutron shielding is the production of gamma radiation, which occurs in the process of neutron attenuation. Consequently, sufficient gamma ray attenuating material must be included in the shield arrangement to minimize the escape of these gamma rays from the shield. Since, like gamma rays, neutrons are scattered in the attenuation process, a shield that provides protection in all directions is necessary.

In general, concrete or damp earth represents a fair compromise for neutron and for gamma ray shielding. Although these materials do not normally contain elements of high atomic weight, they do have a fairly large proportion of hydrogen—for the purpose of slowing down and capturing neutrons—as well as calcium, silicon, and oxygen to absorb the gamma radiations. For example, a thickness of 254 mm (10 in.) of concrete will decrease the integrated neutron flux by a factor of about 10; and 508 mm (20 in.), by a factor of roughly 100. Gamma radiation would be decreased to a somewhat lesser extent, but in sufficient thickness, concrete could be used to provide shielding against both neutrons and gamma rays. Damp earth will act in a similar manner, although a thickness about 50% greater would be required.

An increase in the absorption of the nuclear radiations

can be achieved by using a modified ("heavy") concrete made by adding a considerable proportion of an iron (oxide) ore—e.g., limonite—to the mix and incorporating small pieces of iron such as steel punchings. Alternatively, the mineral barytes, a compound of barium, may be included in the concrete. The presence of a heavy element such as iron or barium improves the neutron and gamma ray shielding properties of any given thickness (or volume) of the material. Attenuation of the integrated neutron flux by a factor of 10 requires about 178 mm (7 in.) of this heavy concrete.

The addition of boron or a boron compound to neutron shields has certain advantages. The lighter isotope (boron-10) of the element captures slow neutrons very readily and, in the process, emits gamma rays of moderate energy (0.48 MeV) that are not difficult to attenuate. Thus the mineral colemanite, which contains a large proportion of boron, when incorporated into concrete, will improve the ability of the concrete to absorb neutrons.

10-8.2 NONIONIZING RADIATION

Nonionizing radiation, as its name implies, is radiation that does not ionize body tissue or other materials in its path. However, this radiation does produce other damaging effects discussed in the paragraphs that follow. Nonionizing radiations include those in the electro-magnetic regions ranging from radio waves to ultraviolet. Included in this category are microwave, infrared, visible, laser, and ultraviolet radiation. (For the extent of this electromagnetic spectrum, see Fig. 10-21.) Laser-generated radiation is such a rapidly growing field that a separate subparagraph, par. 10-8.2.4, is devoted to laser safety.

10-8.2.1 Ultraviolet Radiation

Ultraviolet radiation produces thermal or photo-chemical injuries. The sun is the most common source of ultraviolet radiation; the principal artificial source is electrical welding. Other sources include ultraviolet (sun-tanning) lamps, mercury vapor-type streetlights, and plasma torches (welding using electric arcs).

The parts of the body most vulnerable to ultraviolet energy are the cornea and conjunctiva of the eye; they become irritated and inflamed and respond with excessive tearing. These effects may not appear until 6 to 12 h later, particularly with mild exposures. Experiments have shown that there is little temperature rise in the affected areas to provide warnings of damage. The adverse effects appear to be photochemical, rather than thermal, in nature. The biological feeling is much like having fine sand mixed in the eyes.

Protection against ultraviolet radiation is easy to provide; any opaque cover, even if very thin, will absorb ultraviolet radiation. In addition, ultraviolet radiation from any source can be absorbed by suitable sunburn prevention creams. Exposure to ultraviolet radiation is cumulative over the short term. Protective glasses for the eyes and creams for the exposed parts of the head and neck—or face masks and protective clothing for the rest of the body—should provide complete protection against the worst possible exposure to ultraviolet radiation.

Ultraviolet radiation also affects materials. It can degrade polymers. Photochemical processes cause the breakdown of such polymers as natural and synthetic rubber, vinyl chloride, and vinylidene chloride, which releases hazardous hydrogen chloride. The hydrogen chloride, an acid, causes further breakdowns such as crazing and cracking, and the degradation of desirable physical and electrical properties. If any of these polymers are expected to receive ultraviolet radiation, they should be adequately shielded to prevent degradation. Useful shielding techniques consist of painting (white paint offers superior protection), covering with an opaque material or impregnating the polymeric material with dyes. The principal wavelength of the ultraviolet radiation should be determined, if possible, and shielding offering maximum protection against that wavelength should be provided.

Tires and other rubber or plastic parts on Army equipment that deteriorate under ultraviolet radiation should be replaced periodically if exposed to the sun. Exposed equipment fabricated from composite materials with epoxy binders should be protected with paints that minimize the heat input to the equipment to minimize degradation of the composite materials.

10-8.2.2 Infrared Radiation

All objects radiate infrared radiation; it is absorbed by other bodies with lower temperatures. Infrared (IR) radiation is electromagnetic in nature, and it is easily converted to heat when it strikes another body. The injurious effects of IR include all of those possible from heat or high temperatures. Skin burns are the principal effect. Continued whole-body exposure to intense infrared radiation can cause excessive perspiration and loss of body salts; this, in turn, could result in heat exhaustion, heat stroke, or heat cramps. Localized exposure to infrared radiation is not likely to induce these effects but could cause localized blistering.

The eyes, which are very sensitive to all forms of radiation, are readily damaged by intense IR. Recent research indicates that such exposure may cause cataracts, in which the lens of the eye gradually becomes opaque so that vision is lost. The retina is also susceptible to IR damage because the lens and cornea focus the energy into a very small area on the retina and, thereby, increase the intensity of irradiation.

The most hazardous source of IR is the laser. A detailed description of laser radiation is provided in par. 10-8.2.4.

10-8.2.3 Microwave Radiation

Absorption of microwave radiation by the body increases the kinetic energy of the absorbing molecules; this energy manifests itself as heat. The chief hazard lies in the inability of an organ to dissipate the heat created by the absorbed microwave energy. When that heat cannot be adequately dissipated, the temperature of the organ will rise and cause the possible burning of sensitive tissues. Although internal heating is the primary hazard, the adverse psychological hazards of microwave absorption may be more serious than previously thought. The resulting symptoms such as nervousness and irritability indirectly affect the safety of the person. The possibility of microscopic, biochemical, and cataract-producing effects from microwave radiation is still under investigation. An exhaustive paper on the human exposure to nonionizing radiant energy, potential hazards, and safety standards (Ref. 47) provides much background data on this subject.

Studies performed by the Bureau of Radiological Health have shown that microwave power densities below 1000 W/m^2 at 1.2 to 24.2×10^9 Hz do not affect the body thermally. Therefore, with a safety factor of 10, the permissible level of exposure was set at 100 W/m^2. Some sensitive areas of the skin, however, will feel pain even at low intensities, e.g., 200-600 W/m^2 for 1 s, at certain frequencies. TB MED 253 (Ref. 48) sets exposure limits in areas subjected to microwave radiation. These limits are given in Table 10-26.

The values in Table 10-26 apply to whole- or partial-body exposure of continuous or intermittent duration averaged over any 0.1-h period.

Sources of microwave radiation—e.g., high-powered radars, control and track radars, airborne radar, microwave and other communications systems, alarm systems, and signal generators—are found throughout the Army. Klystrons, magnetrons, and high-frequency and solid-state devices are also all sources of microwaves.

High-intensity microwave fields can cause inductive heating of metals and can cause sparks. Rings and other jewelry worn by personnel can be heated in these strong fields and can cause serious burns. Metal containers can become hot enough to ignite flammable or explosive materials.

Certain configurations of electric wires or metal parts can act as antennas to induct radar or radio frequencies. These components can develop voltages high enough to

arc or spark and thus constitute a source of ignition for any flammable materials in the same area.

Nearby personnel can often be protected from microwave radiation by means of shielding. The most effective and practical shielding is made of an electrically conductive material, as indicated by the information in Table 10-27 (Ref. 48). Solid foils of various conducting materials can be used to enclose the microwave source as in microwave ovens. The foil shielding can also be used to enclose sensitive electronic units, such as computers, to protect them from unknown radiation fields.

It may not be possible to provide shielding for some radar and microwave communications equipment. There are other methods, however, when shielding is not possible. Interlocks can prevent inadvertent activation of microwave radiators. Dummy loads should be used to absorb microwave energy during tests in closed areas. Equipment that radiates microwave energy should be clearly marked with warning labels to advise of the hazard, and radiation areas should be posted with warning signs. The following measures can be taken to protect users and maintenance personnel:

1. No microwave antenna or other emitter should be inspected or serviced when energized.

2. Dummy loads should be used whenever possible to absorb the energy output of transmitting microwave equipment while it is being adjusted, checked, or tested.

3. Operating microwave radiators should not be aimed at inhabited areas or personnel.

4. Rings, watches, keys, or other metallic objects should not be worn or carried by personnel working in areas where there might be microwave radiation, even radiation of low intensity.

5. Tools or other metallic objects that might have received microwave radiation should be grasped carefully because they may be hot.

6. Flammable or explosive materials in contact with metallic containers should not be exposed to microwave radiation.

7. Each piece of microwave equipment should be equipped with a warning device to indicate when it is radiating. These devices should provide both aural and visual warnings. Passive warning signs should be designed as shown in Fig. 10-23 (Ref. 48).

8. Techniques, warnings, and cautions of the military handbooks on the hazards of electromagnetic radiation to ordnance (HERO) should be observed. HERO guidance requires

    a. Determining the radiation level that can initiate the ordnance item or other flammable materials

    b. Insuring that the radiation levels in the vicinity of ordnance are never allowed to exceed the safe level, i.e., the ordnance initiation levels minus a safety factor.

Additional information of use to designers can be found in par. 10-8.6.

TABLE 10-26. EXPOSURE LIMITS TO MICROWAVE RADIATION (Ref. 48)

Power Density, W/m^2	Exposure
100	Unlimited
100-500	Limited
Above 500	Denied

TABLE 10-27. SHIELDING MATERIALS AND ATTENUATION (Ref. 48)

Materials	dB Attenuation			
	Frequency (GHz)			
	1-1.5	2.5-3.5	4.5-6.0	8-12
60×60 mesh screening	20	25	22	20
32×32 window mesh	18	22	22	18
0.25 mesh (hardware cloth)	18	15	12	10
Window glass	2	2	3	3.5
19-mm (0.75-in.) pine sheathing	2	2	2	3.5
203-mm (8-in.) concrete wall (solid)	20	22	26	30

Proportions

M	D
2.70	0.05
4.00	0.074
5.40	0.10
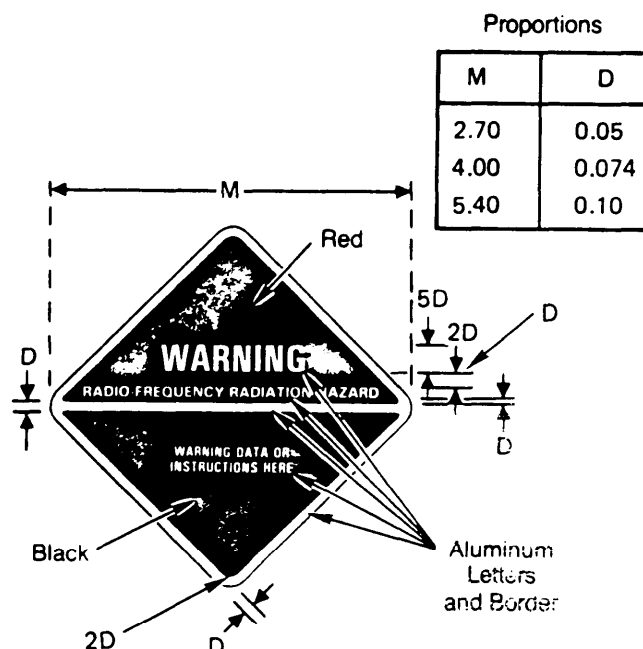
Figure 10-23. RF Radiation Hazard Sign (Ref. 48)

10-8.2.4 Laser Radiation

Lasers (Light Amplification by the Stimulated Emission of Radiation) are devices that generate and emit coherent light. The laser is a very useful tool for the Army. It is used in target designators, range finders, guidance systems, and other applications where a coherent source of light is required or beneficial. The widespread use of laser systems increases the probability of personnel exposure to injurious levels of laser radiation. Although lasers have characteristics that can be used to good advantage, they are potentially hazardous and safeguards must be provided.

The coherent light emitted by a laser is optical, monochromatic radiation emitted at one frequency, in phase (no interference). The laser emits an extremely high-energy beam with little dispersion. The intensity of the emitted energy can be far greater than is available from any other source of high-intensity light. The bright-

ness exceeds all known natural and man-made light sources.

Depending upon the type, lasers can radiate in infrared, visible, and ultraviolet regions of the spectrum. The beam from an infrared or ultraviolet laser may be invisible to the naked eye; consequently, it may go unnoticed and thus increase the potential for injury. Even if the light output from a laser is less than that from an ordinary incandescent lamp (100 W), the coherent character of the laser will result in extremely high irradiance, i.e., power per unit area, in a cross section of its beam.

Injury, however, is not limited to the radiation effects of the emitted beam. The equipment associated with the laser system, including the target, are also hazard sources, i.e.,

1. Electrical shock and/or burn hazard associated with high voltages and charged condenser banks

2. X rays produced from high-voltage vacuum tubes used in laser power supplies or from electric discharge lasers

3. Chemical burn, toxic, and corrosion hazards associated with highly toxic and corrosive materials used in laser research laboratories

4. Toxic atmosphere resulting from target vaporization

5. Miscellaneous mechanical, fire, and noise hazards associated with or resulting from the laser system

6. Cryogenic fluids used for cooling. When cryogenic fluids evaporate, they displace breathable oxygen. Consequently, good ventilation is required.

These hazards will be discussed in the paragraphs that follow.

Laser radiation produces the same kinds of injuries as any other infrared or ultraviolet radiation, i.e., either thermal or photochemical. Fig. 10-24 (Ref. 49) shows that laser wavelengths across the ultraviolet, visible, and infrared bands can cause burns. The more serious skin penetration occurs at the wavelengths near 1080 nm. Lasers can burn exposed skin; the powerful ones can also result in injury if the beam is reflected from a shiny (specular) surface. Some diffuse reflections can also be hazardous.
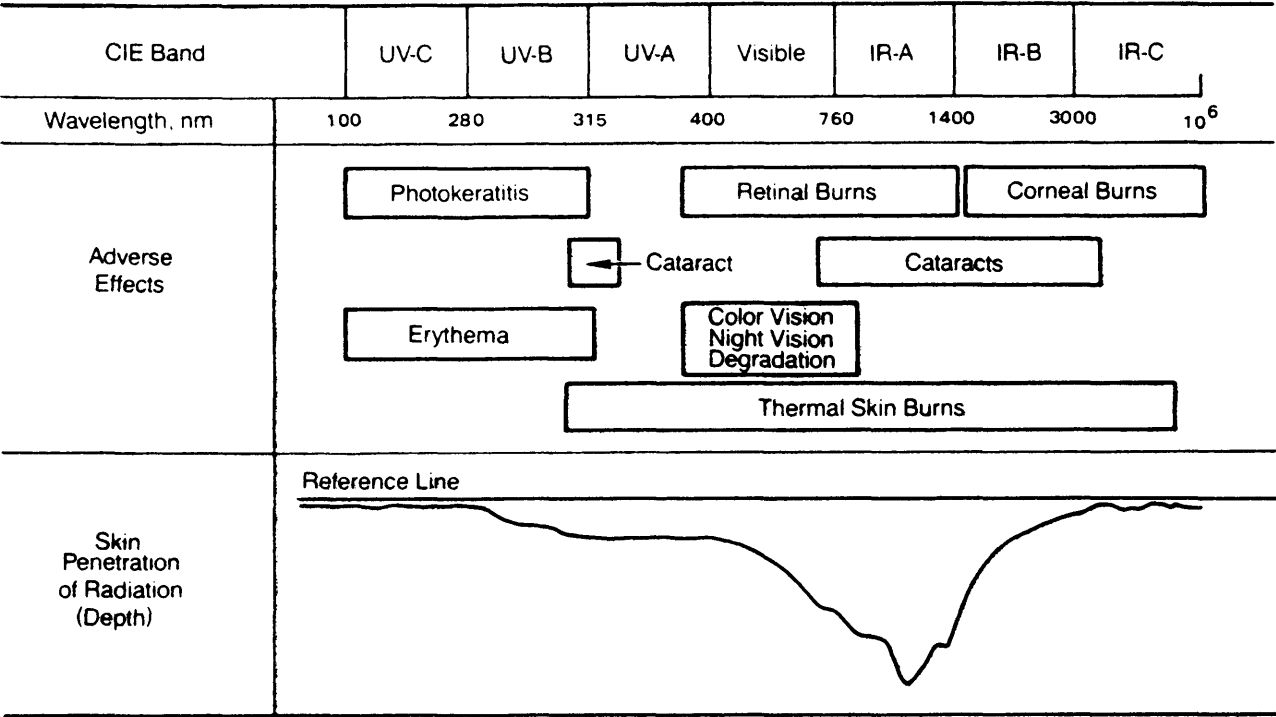
CIE Band	UV-C	UV-B	UV-A	Visible	IR-A	IR-B	IR-C

Wavelength, nm   100   280   315   400   760   1400   3000 10^6

Figure 10-24. Spectral Bands of Optical Radiation and Effects on the Human Body (Ref. 49)

The eye is very susceptible to damage from laser radiation because the radiance, i.e., radiant power output per unit solid angle per unit area (Ref. 9), in a laser beam is very high. The eyes can react very quickly—a blink reflex is 0.25 s (Ref. 50)—to certain frequencies of light, but due to the intense energies in a laser beam, they may not react quickly enough to prevent damage. In addition, the two protective mechanisms—the eyelid and/or the iris—may not react to the specific frequencies of some lasers. The result can be radiation damage to the cornea, the lens, and the retina—or the whole eye—and possible permanent loss of vision, depending upon the frequency and intensity of the laser and the exposure time. The effect of rapid thermal heating or actinic (photochemical) changes, even when temporary, can cause extreme pain.

To provide a laser that can be used safely, a number of safeguards to minimize its inherent hazards should be considered during the design. To assist the laser designers and operators, groups of lasers have been categorized according to their capability to cause injury. A brief discussion of the categories follows (Ref. 9):

1. *Class 1, or "Exempt" Lasers.* This group normally is limited to gallium-arsenide lasers and is not considered hazardous.

2. *Class 2.* This group is often referred to as "low-power" or "low-risk" laser systems that are considered hazardous only if the viewer overcomes his or her natural average response to bright light and continuously stares into the source.

3. *Class 3.* This group is referred to as "medium-power" or "moderate-risk" laser systems that can cause injury within the natural aversion response time, i.e., faster than the blink of an eye.

4. *Class 4.* This group is referred to as "high-power" or "high-risk" laser systems that can cause significant injury and cause combustion of flammable materials. These systems may also cause injury due to diffuse reflections. The average power output is 500 mW or greater.

In deciding on the laser classification for those lasers that can potentially emit at various wavelengths, the classification shall be based on the most hazardous possible operation.

The categories outlined in the previous paragraph are more carefully defined, and exposure limits established, by TB MED 524 (Ref. 9). Excerpts from par. D-5, Appendix D, (Ref. 9) follow:

"a. *Class 1.* Any laser device that cannot emit laser radiation levels in excess of the AEL [accessible emission limit] for the maximum possible duration inherent to the design of the laser or laser system. The exemption from hazard controls strictly applies to emitted laser radiation hazards and not to other potential hazards.

"b. *Class 2.*

(1) Visible (400 nm to 700 nm) CW [continuous wave] laser devices that can emit a power exceeding the AEL for Class 1 for the maximum possible duration inherent to the design of the laser or laser system but not

exceeding 1 mW.

(2) Visible (400 nm to 700 nm) repetitively pulsed laser devices that can emit a power exceeding the appropriate AEL for Class 1 for the maximum possible duration inherent to the design of the laser device but not exceeding the AEL for a 0.25 s exposure.

"c. *Class 2a*. A visible (400 nm to 700 nm) laser or laser system that is not intended for intrabeam viewing and does not exceed the exposure limit for 1000 s of viewing time.

"d. *Class 3a*. Class 3a lasers or laser systems have—

(1) An accessible output power or energy between 1 and 5 times the lowest appropriate AEL for Class 2 for visible wavelengths, and between 1 and 5 times the AEL for Class 1 for all other wavelengths.

(2) Do not exceed the appropriate exposure levels as measured over the limiting aperture (2.5 mW·cm^{-2} for visible CW lasers).

"e. *Class 3b*.

(1) *Infrared (1.4 μm to 1 mm) and ultraviolet (200 nm to 400 nm) laser devices*. Emit a radiant power in excess of the AEL Class 1 for the maximum possible duration inherent to the design of the laser device. Cannot emit an average radiant power of 0.5 W or greater for T_{max} [maximum duration of daily exposure inherent in the design of the laser device] greater than 0.25 s, or a radiant exposure of 10 J·cm^{-2} within an exposure time of 0.25 s or less.

(2) *Visible (400 nm to 700 nm) CW or repetitive pulsed laser devices*. Produce a radiant power in excess of the AEL Class 1 for a 0.25 s exposure (1 mW for a CW laser). Cannot emit an average radiant power of 0.5 W or greater for T_{max} greater than 0.25 s.

(3) *Visible and near-infrared (400 nm to 1400 nm) pulsed laser devices*. Emit a radiant energy in excess of the AEL Class 1. Cannot emit a radiant exposure that exceeds that required to produce a hazardous diffuse reflection as given in table D-1 [Table 10-28].

(4) *Near-infrared (700 nm to 1400 nm) CW laser devices or repetitively pulsed laser devices*. Emit power in excess of the AEL for Class 1 for the maximum duration inherent in the design of the laser device. Cannot emit an average power of 0.5 W or greater for periods in excess of 0.25 s.

"f. *Class 4*.

(1) *Ultraviolet (200 nm to 400 nm) and infrared (1.4 μm to 1 mm) laser devices*. Emit an average power of 0.5 W or greater for periods greater than 0.25 s, or a radiant exposure of 20 J·cm^{-2} within an exposure duration of 0.25 s or less.

TABLE 10-28. MAXIMUM ALLOWABLE RADIANT INTENSITY FROM A DIFFUSE SURFACE REFLECTION AS MEASURED AT THE REFLECTING SURFACE FOR EXTENDED SOURCES: ANGULAR SUBTENSE α_{min}* (Ref. 9)

Duration of Exposure, s	Exposure Limit at Cornea, J·cm^{-2}sr^{-1} (See Fig. 10-27 for graphic presentation of this column.)	Limiting Angle α_{min}, mrad (See Fig. 10-29.)	Permissible Laser Beam Radiant Exposure Incident on Diffuse Reflecting Surfaces, J·cm^{-2} (Values in columns 4, 5, 6 = values in column $2 \times \pi / \rho$.)		
			Reflectance $\rho = 1$	Reflectance $\rho = 0.50$	Reflectance $\rho = 0.10$
1	2	3	4	5	6
10^{-9}	1.0×10^{-2}	8.0	3.1×10^{-2}	6.3×10^{-2}	3.1×10^{-1}
10^{-8}	2.2×10^{-2}	5.4	6.9×10^{-2}	1.4×10^{-1}	6.9×10^{-1}
10^{-7}	4.6×10^{-2}	3.7	1.5×10^{-1}	2.9×10^{-1}	1.5
10^{-6}	1.0×10^{-1}	2.5	3.1×10^{-1}	6.3×10^{-1}	3.1
10^{-5}	2.2×10^{-1}	1.7	6.9×10^{-1}	1.4	6.9
10^{-4}	4.6×10^{-1}	2.2	1.5	2.9	15
10^{-3}	1.0	3.6	3.1	6.3	31
10^{-2}	2.2	5.7	6.9	14	69
10^{-1}	4.6	9.2	15	29	145
1	10	15	31	63	314
10 to 10^4	22	24	69	138	691

Note:

   The actual radiant exitance (the light reflected from a diffuse surface) may be calculated by multiplying the radiant exposure or irradiance of the beam impinging upon the surface by the reflectance (a property of the material). These values may be approximately tripled for conditions of bright ambient light.

Typical diffuse reflection cases for visible radiation ($C_A = 1$ for λ = 400 to 700 nm) (For wavelengths between 0.7 and 1.4 μm, use appropriate correction factors from Fig. 10-30.)

*Exposure limits for extended sources apply to sources that subtend an angle greater than α_{min}—the minimum angle subtended by a source for which extended source exposure limit applies—that varies with exposure duration. This angle is not the beam divergence of the sources.

(2) *Visible (400 nm to 700 nm) and near-infrared (700 nm to 1400 nm) [0.7 μm to 1.4 μm] laser devices.* Emit an average power of 0.5 W or greater for periods greater than 0.25 s, or a radiant exposure in excess of that required to produce a hazardous diffuse reflection as given in table D-1 [Table 10-28]."

Tables 10-29, 10-30, and 10-31 (Ref. 9) provide a complete list of laser exposure limits (ELs). These ELs are the maximum permissible exposures under conditions to which nearly all personnel may be exposed without adverse effects. The values are guides in the control of exposures and should not be regarded as fine lines between safe and dangerous levels. Figs. 10-25 through 10-34 (Ref. 9) provide graphs of exposure limits that may be too difficult to calculate. Appendix E of Ref. 9 has many solved examples of the determination of applicable ELs and laser classifications.

TABLE 10-29. EXPOSURE LIMITS FOR DIRECT OCULAR EXPOSURES (INTRABEAM VIEWING) FROM A LASER BEAM (Ref. 9)

Spectral Region	Wavelength, nm	Exposure time, † s	Exposure Limit	Defining Aperature, mm
UV-C	200-302	10^{-9}-3×10^{4}	3 mJ·cm^{-2}	1
UV-B	303	10^{-9}-3×10^{4}	4 mJ·cm^{-2}	1
	304	10^{-9}-3×10^{4}	6 mJ·cm^{-2}	1
	305	10^{-9}-3×10^{4}	10 mJ·cm^{-2}	1
	306	10^{-9}-3×10^{4}	16 mJ·cm^{-2}	1
	307	10^{-9}-3×10^{4}	25 mJ·cm^{-2}	1
	308	10^{-9}-3×10^{4}	40 mJ·cm^{-2}	1
	309	10^{-9}-3×10^{4}	63 mJ·cm^{-2}	1	or 0.56$t^{1/4}$ J·cm^{-2}
	310	10^{-9}-3×10^{4}	100 mJ·cm^{-2}	1
	311	10^{-9}-3×10^{4}	160 mJ·cm^{-2}	1
	312	10^{-9}-3×10^{4}	250 mJ·cm^{-2}	1
	313	10^{-9}-3×10^{4}	400 mJ·cm^{-2}	1
	314	10^{-9}-3×10^{4}	630 mJ·cm^{-2}	1
UV-A	315-400‡	10^{-9}-10	0.56$t^{1/4}$ J·cm^{-2}	1
	315-400	10-10^{3}	1.0 J·cm^{-2}	1
	315-400	10^{3}-3×10^{4}	1.0 mW·cm^{-2}	1
Light	400-700	10^{-9}-1.8×10^{-5}	5×10^{-7} J·cm^{-2}	7
	400-700	1.8×10^{-5}-10	1.8$t^{3/4}$ mJ·cm^{-2}	7
	400-550	10-10^{-4}	10 mJ·cm^{-2}	7
	550-700	10-T_1	1.8$t^{3/4}$ mJ·cm^{-2}	7
	550-700	T_1-10^{4}	10 C_B mJ·cm^{-2}	7
	400-700	10^{4}-3×10^{4}	$C_B\mu$W·cm^{-2}	7
IR-A	701-1049	10^{-9}-1.8×10^{-5}	5 $C_AC_P\times10^{-7}$ J·cm^{-2}	7
	701-1049	1.8×10^{-5}-10^{3}	1.8 $C_At^{3/4}$ mJ·cm^{-2}	7
	1050-1400	10^{-9}-5×10^{-5}	5 $C_P\times10^{-6}$ J·cm^{-2}	7
	1050-1400	5×10^{-5}-10^{3}	9$t^{3/4}$ mJ·cm^{-2}	7
	701-1400	10^{3}-3×10^{4}	320 C_A μW·cm^{-2}	7
IR-B&C	1.4-10^{3} μm†	10^{-9}-10^{-7}	10^{-2} J·cm^{-2}	1,11*
	1.4-10^{3} μm†	10^{-7}-10	0.56$t^{1/4}$ J·cm^{-2}	1,11*
	1.4-10^{3} μm	>10	0.1 W·cm^{-2}	1,11*

*1mm for 1400-10^{5} nm; 11 mm 10^{5}-10^{6} nm

†The exposure limit at 1540 (Erbium) for a single-pulse exposure (< 1 μs) is 1 J·cm^{-2}

‡or not to exceed 1 J·cm^{-2} over 24 h.

Notes:
1. To aid in the determination of exposure limits for exposure durations requiring calculations of fractional powers, Figs. 10-25 through 10-29 may be used.
2. Correction Factor $C_A = 10^{[0.002(\lambda - 700)]}$ for λ = 700-1049 nm; $C_A = 1$ for λ = 400-700 nm; $C_A = 5$ for λ = 1050-1400 nm. (See Fig. 10-30.)

TABLE 10-29 (cont'd)

3. Correction Factor $C_B = 1$ for $\lambda = 400\text{-}550$ nm. (See Fig. 10-34.)

4. Correction Factor $C_B = 10^{|0.015(\lambda - 550)|}$ for $\lambda = 550\text{-}700$ nm.

5. $T_1 = 10 \times 10^{|0.020(\lambda - 550)|}$ for λ 550-700 nm.

6. Pulsed Correction Factor $C_p = 1/\sqrt{F}$ for pulse repetition frequency (PRF) ≤ 100 Hz; see Fig. 10-31 for PRFs from > 100 Hz $\leq$ 1000 Hz; $C_p = 0.06$ for PRFs > 1000 Hz. These values of C_p only apply for $t \leq 10$ μs. For $t > 10$ μs, see Note 7.

7. Repetitively Pulsed Lasers. Due to the wide variety of pulsed laser systems and the relative lack of biological data for some spectral regions, caution shall be used in the evaluation of such exposures. Exposure to a scanning laser system may also be evaluated as a series of pulses received by the eye or skin. The exposure limit for irradiance or radiant exposure may be determined by the following guidelines:

   a. Pulsed lasers having a duration less than 10 μs:

     (1) Determine the exposure limit for a single pulse in the pulse train.

     (2) Determine the repetitively pulsed correction factor C_p based on the minimum pulse-to-pulse spacing in time from Fig. 10-31.

NOTE
For PRFs of 1 to 100 Hz, C_p equals the inverse of the square root of the PRF.

     (3) An alternative approach to calculating C_p should be used only when calculating the exposure to a series of pulses lasting less than 10 s. Using a value of C_p equal to the inverse of the fourth root of the total maximum number of pulses n, a person might receive in a 10-s period of time $C_p = n^{-1/4}$.

     (4) A complicated series of pulses lasting longer than 10 s may have a C_p calculated from Fig. 10-31 based on the average PRF.

     (5) All pulses emitted within 18 μs should have their energies added and counted as one pulse.

     (6) All groupings of pulses from 18 μs to the maximum exposure duration a person would reasonably be expected to receive should have an emission limit calculated separately. Calculate the emission limit as if each group of pulses were actually one pulse with a pulse duration equal to the duration of the group of pulses. The single-pulse emission limit is then determined by dividing the emission limit for the group by the number of pulses in the group. Of those calculated, the most conservative (lowest value) single-pulse emission limit should be used.

   b. Pulsed lasers having a duration greater than 10 μs:

     (1) Determine the total number of pulses n in an individual exposure. A 10-s time period may be used in most cases when the exact exposure time is unknown.

     (2) Multiply the number of pulses by the length of each pulse nt.

     (3) Determine the exposure limit $EL_{(nt)}$ for a pulse duration of nt.

     (4) Determine the single-pulse exposure limit $EL_{(single\,pulse)}$ by dividing the exposure limit determined above by any number of pulses as shown by the following equation:

$$EL_{(single\,pulse)} = \frac{EL_{(nt)}}{n}$$

TABLE 10-30. EXPOSURE LIMITS FOR VIEWING A DIFFUSE REFLECTION OF A LASER BEAM OR AN EXTENDED SOURCE LASER (Ref. 9)

Spectral Region	Wavelength, nm	Exposure Time t, s	Exposure Limit
Light	400-700	$10^{-9}\text{-}10$	$10t^{1/3}$ J·cm^{-2}·sr^{-1}
	400-550	$10\text{-}10^4$	21 J·cm^{-2}·sr^{-1}
	550-700	$10\text{-}T_1$	$3.83t^{3/4}$ J·cm^{-2}·sr^{-1}
	550-700	$T_1\text{-}10^4$	$21C_B$ J·cm^{-2}·sr^{-1}
	400-700	$10^4\text{-}3\times10^4$	$2.1C_B$ mW·cm^{-2}·sr^{-1}
Near infrared	700-1400	$10^{-9}\text{-}10$	$10C_A t^{1/3}$ J·cm^{-2}·sr^{-1}
	700-1400	$10\text{-}10^3$	$3.83C_A t^{3/4}$ J·cm^{-2}·sr^{-1}
	700-1400	$10^3\text{-}3\times10^4$	$0.64C_A$ W·cm^{-2}·sr^{-1}

Note:
C_A, C_B, and T_1 are the same as in footnote to Table 10-29.

TABLE 10-31. EXPOSURE LIMITS FOR SKIN EXPOSURE FROM A LASER BEAM (Ref. 9)

Spectral Region	Wavelength	Exposure Time t, s	Exposure Limit
UV	200 to 400 nm	10^{-9}-3×10^{4}	Same as Table 10-28
Light & infrared A	400 to 1400 nm	10^{-9}-10^{-7}	$2C_A\times10^{-2}$ J·cm^{-2}
do	do	10^{-7}-10	$1.1C_At^{1/4}$ J·cm^{-2}
do	do	10-3×10^{4}	$0.2C_A$ W·cm^{-2}
Infrared B & C	1.4 μm to 1 mm	10^{-9}-3×10^{4}	Same as Table 10-29

Note:

To aid in the determination of exposure limit for exposure durations requiring calculations of fractional powers, Fig. 10-32 may be used. The limiting aperature for all of these ELs is 1 mm for wavelengths less than 0.1 mm. The limiting aperature for wavelengths greater than 0.1 mm is 11 mm.

*Whole-body exposure should be limited to 10 mW·cm^{-2}. The limits in this table refer to a laser beam having a cross-sectional area less than 100 cm^2.
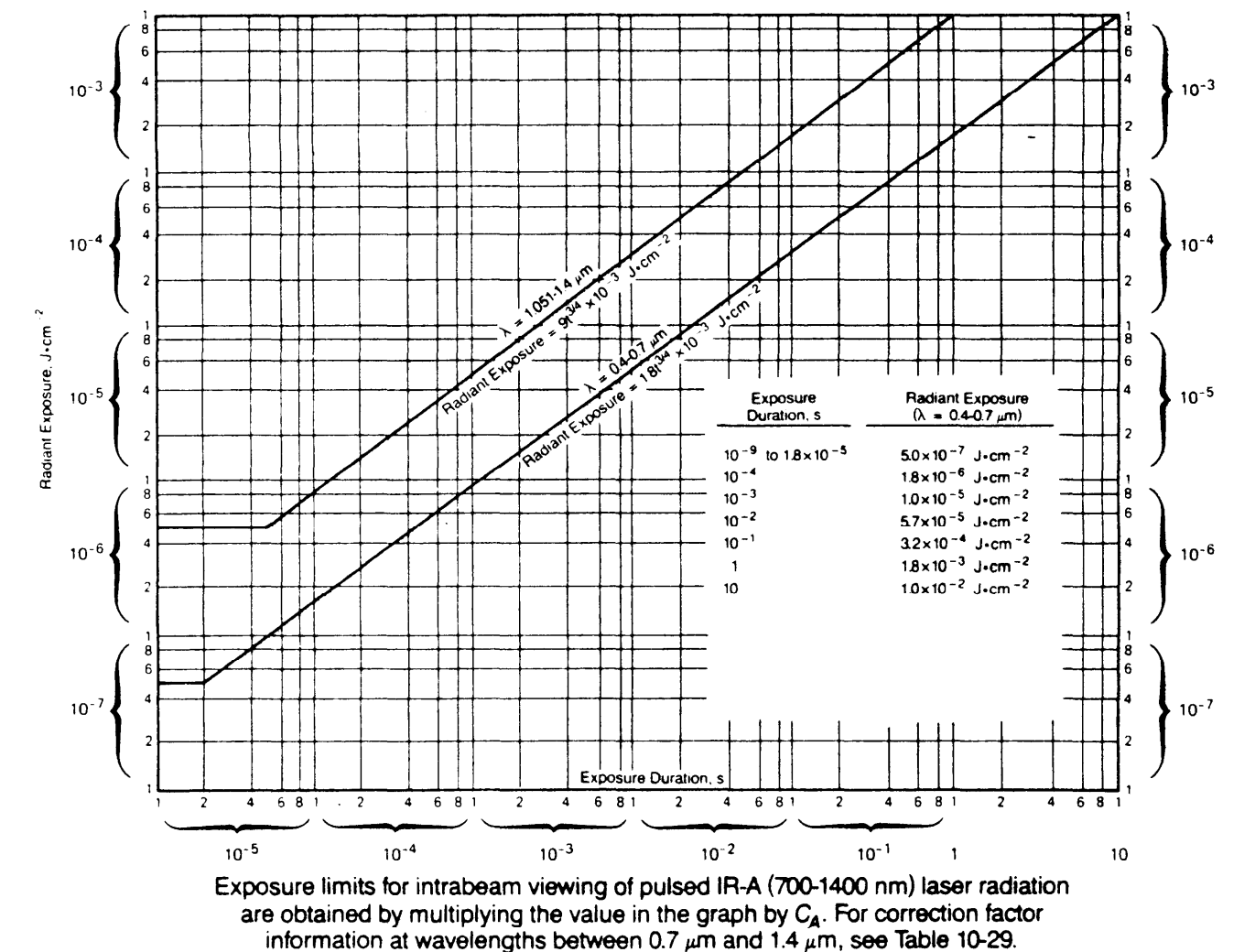
Exposure limits for intrabeam viewing of pulsed IR-A (700-1400 nm) laser radiation
are obtained by multiplying the value in the graph by C_A. For correction factor
information at wavelengths between 0.7 μm and 1.4 μm, see Table 10-29.

Figure 10-25.   Protection Standard for Intrabeam Viewing of Pulsed Visible (400-700 nm) Laser Radiation (Ref. 9)
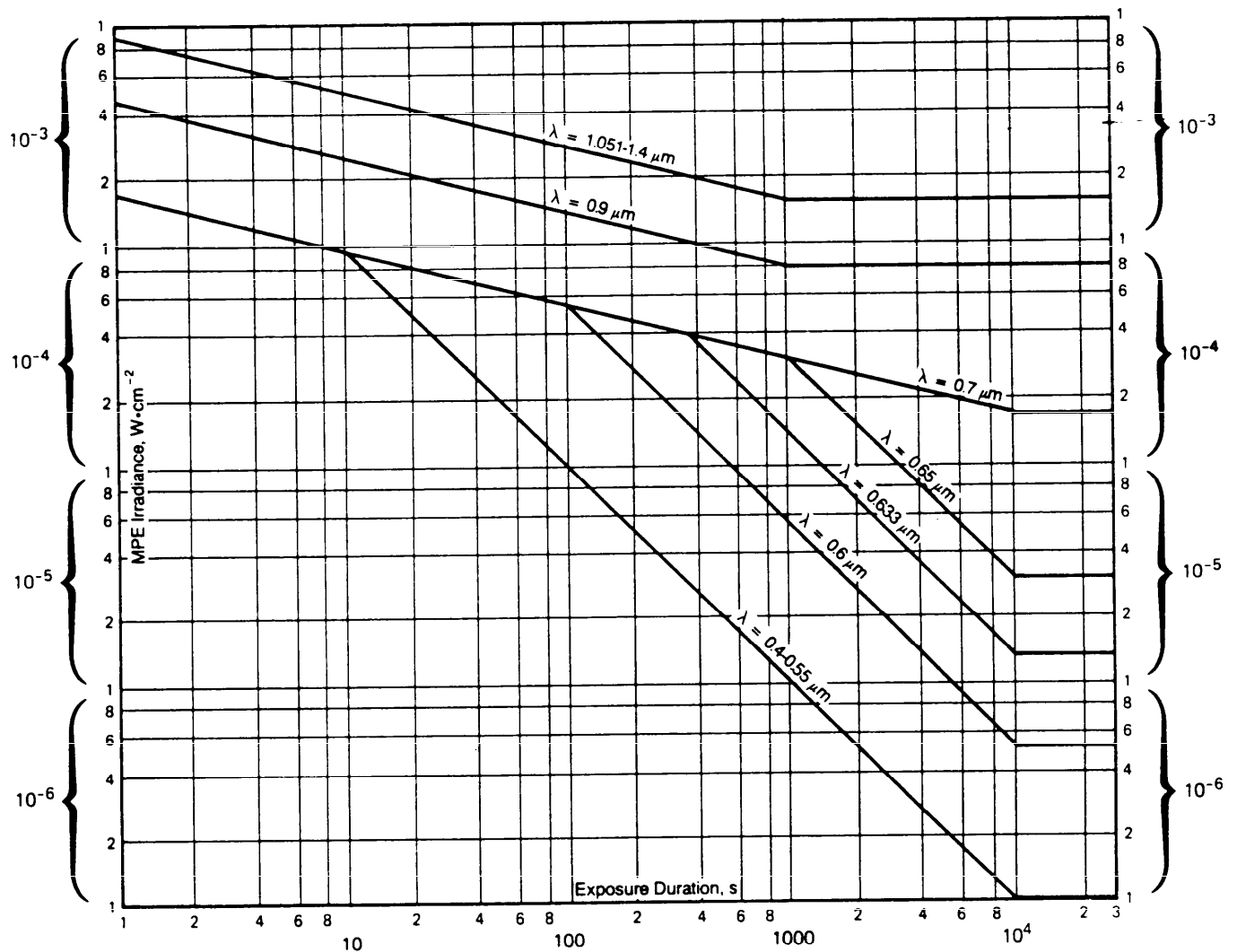
Figure 10-26. Exposure Limit for Intrabeam of CW Visible (400-700 nm) and IR-A (750, 900, and 1060-1400 nm) Laser Radiation (Ref. 9)
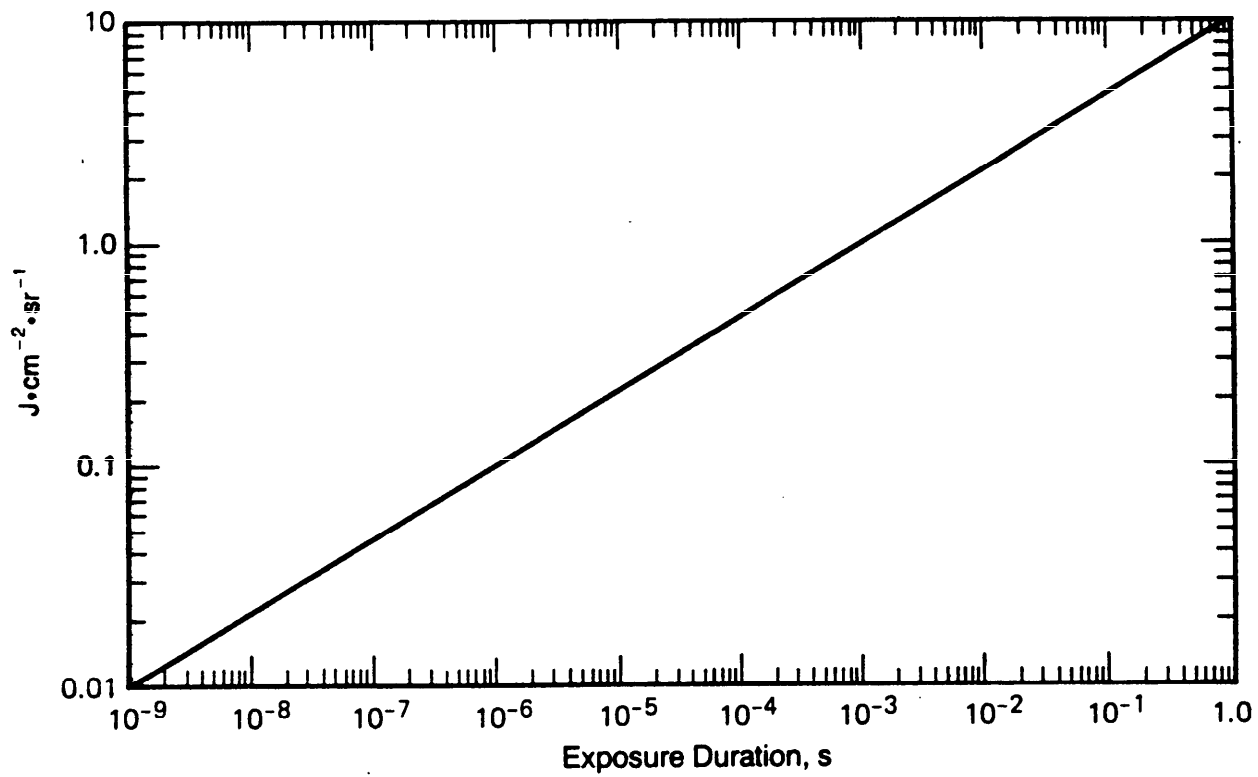
To obtain exposure limit for wavelengths 700-1400 nm, multiply by C_A.

Figure 10-27.   Exposure Limit for Extended Sources or Diffuse Reflections of Pulsed Radiation (400-700 nm) (Ref. 9)
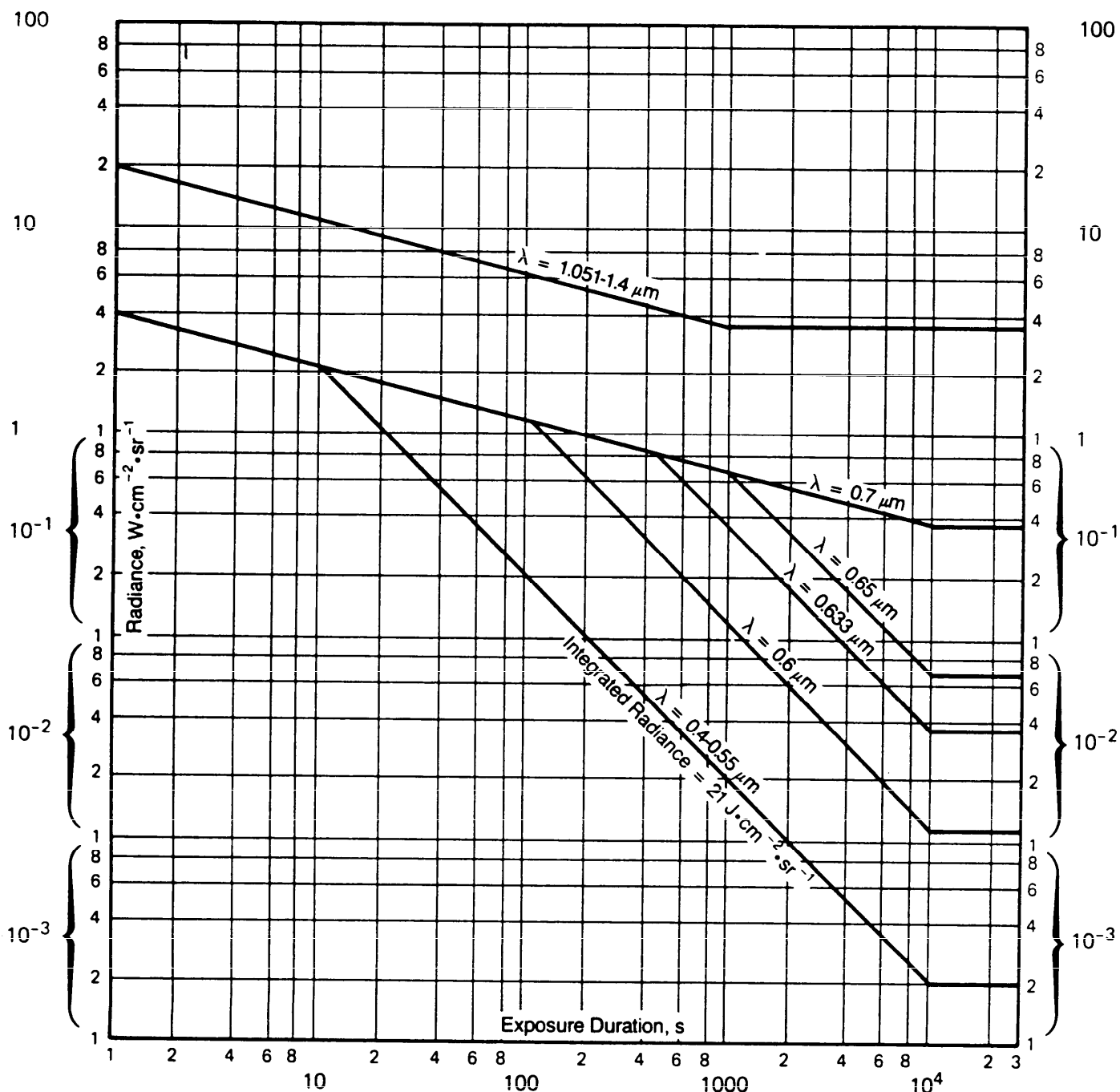
The chart shows:
- Vertical axis (left): Radiance, $W \cdot cm^{-2} \cdot sr^{-1}$
- Horizontal axis: Exposure Duration, s
- Curves labeled: $\lambda = 1.051\text{-}1.4\ \mu m$; $\lambda = 0.7\ \mu m$; $\lambda = 0.65\ \mu m$; $\lambda = 0.633\ \mu m$; $\lambda = 0.6\ \mu m$; $\lambda = 0.4\text{-}0.55\ \mu m$; Integrated Radiance $= 21\ J \cdot cm^{-2} \cdot sr^{-1}$

Figure 10-28.   Exposure Limit for Extended Sources or Diffuse Reflections of CW Visible (400-700 nm) and IR-A (850, 900, and 1060-1400 nm) Laser Radiation (Ref. 9)

The figure contains a table:

Exposure Duration, s	Subtense Angle, mrad λ = 0.4-1.05 μm	Subtense Angle, mrad λ = 1.051-1.4 μm
10^{-9}	8.0	11.3
10^{-8}	5.4	7.7
10^{-7}	3.7	5.4
10^{-6}	2.5	3.7
10^{-5}	1.7	2.5
10^{-4}	2.2	2.2
10^{-3}	3.6	3.6
10^{-2}	5.7	5.7
10^{-1}	9.2	9.2
1	15	15
10 or greater	24	24
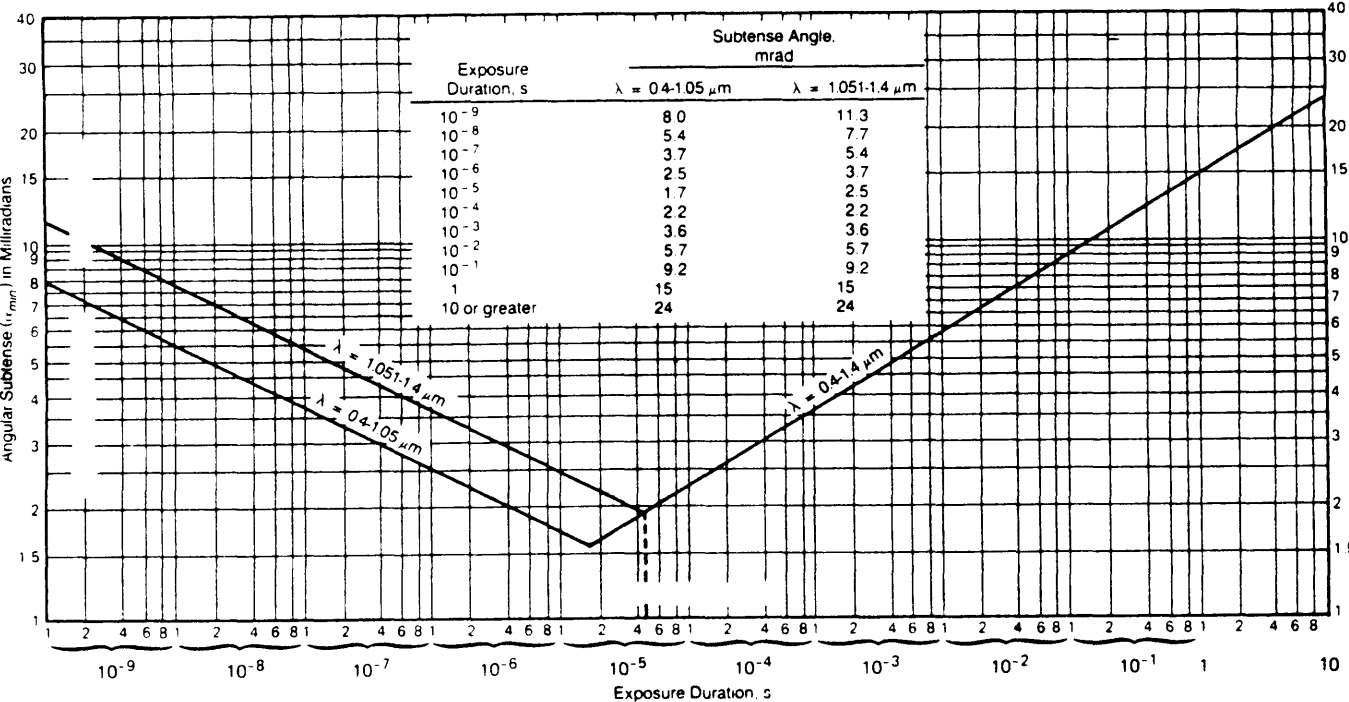
Sources whose angular subtend are less than α_{min} are considered collimated; those greater than or equal to α_{min} are considered extended sources.

Extended sources have an angular subtense or apparent visual angle $\geq \alpha_{min}$. Angular subtenses (apparent visual angles) $< \alpha_{min}$ are considered intrabeam viewing.

Figure 10-29. Limiting Angular Subtense a_{min} of an Extended Source (Ref. 9)
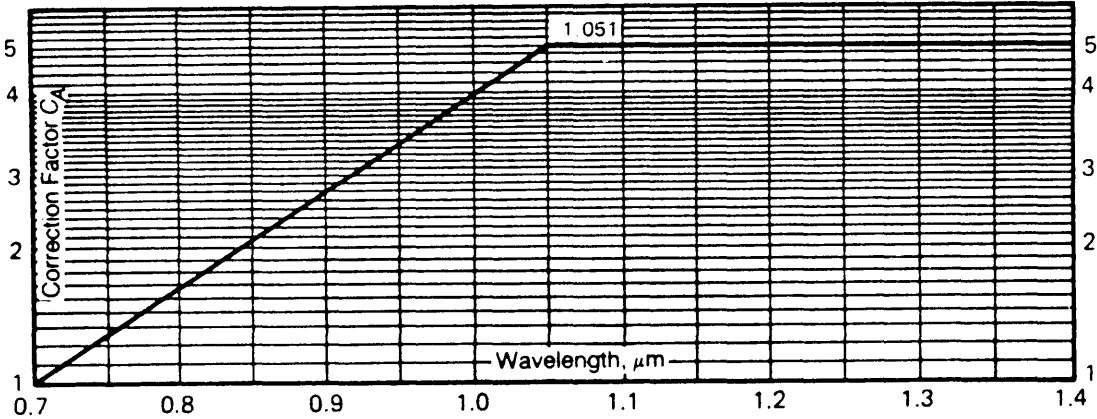
Note: $C_A = 1$ for $\lambda = 0.4$-0.7 μm

$C_A = 10^{2.0(\lambda - 0.7)}$ for $\lambda = 0.7$-1.05 μm

$C_A = 5$ for $\lambda = 1.051$-1.4 μm

Figure 10-30. Correction Factor C_A for Wavelengths 0.7-1.4 μm (Ref. 9)
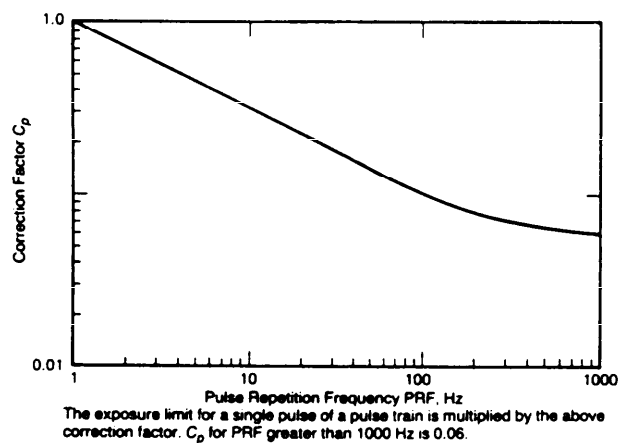
Figure 10-31. Correction Factor C_p for Repetitively Pulsed Lasers Having Pulse Durations Less Than 10^{-5}s (Ref. 9)
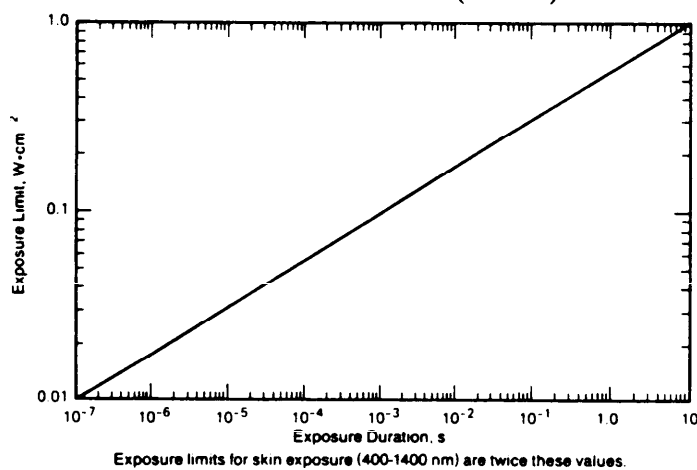
Figure 10-32. Exposure Limit for Pulsed Laser Exposure of Skin and Eyes for Far-Infrared Radiation (Wavelengths Greater Than 1400 nm) (Ref. 9)
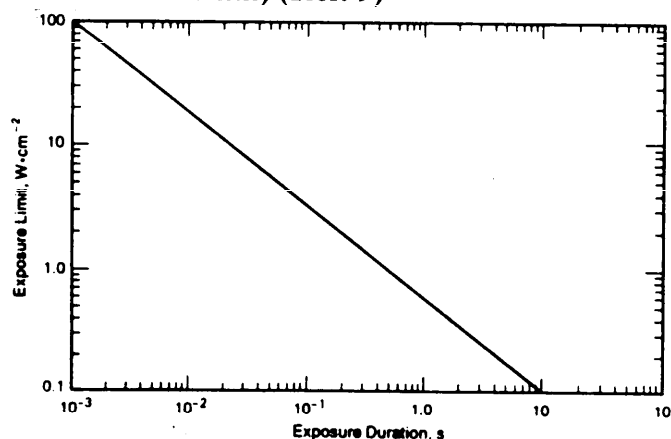
Figure 10-33. Exposure Limit for CW Laser Exposure of Skin and Eyes for Far-Infrared Radiation (Wavelengths Greater Than 1400 nm) (Ref. 9)
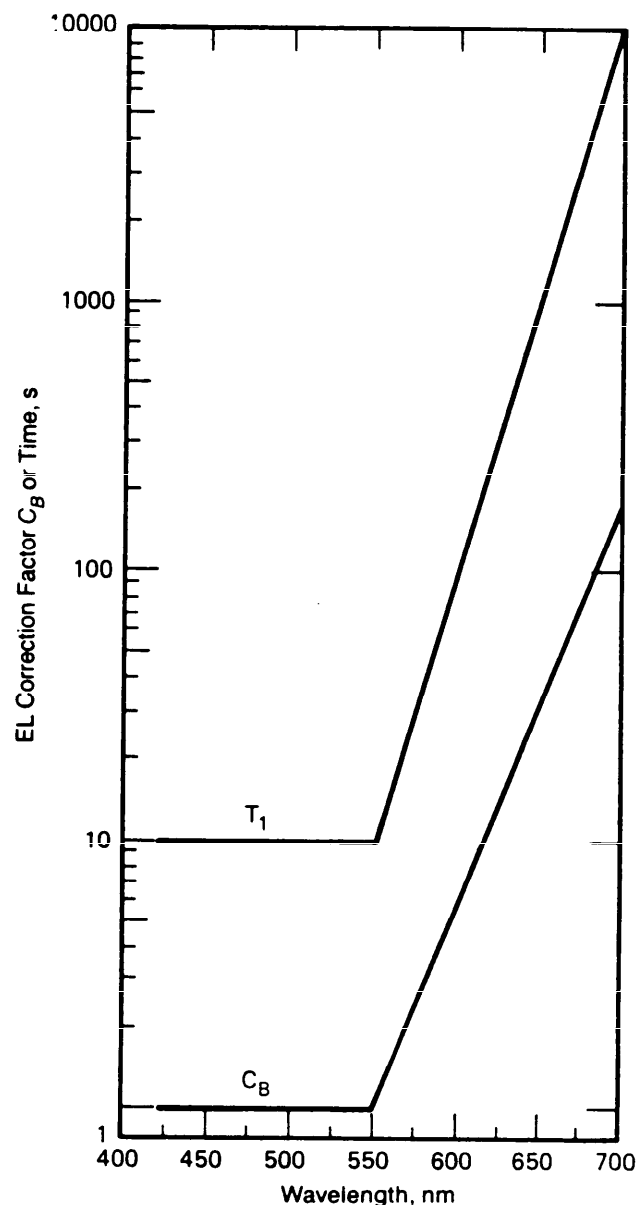
Figure 10-34. Correction Factors C_B and T_1 for Wavelengths 0.55-0.7 μm (Ref. 9)

Because of the increased hazards associated with Class 3 and Class 4 lasers, operations must be conducted in an area controlled by some type of interlock to prevent personnel from entering the path of the beam where beam irradiance exceeds the appropriate protection standard. In addition to this general safety criterion, the interlock system for Class 4 lasers will positively deny personnel access while the laser is capable of operating. Further Class 4 safety requirements are

1. Firing circuits of pulsed lasers will be so designed that they are "fail-safe" to prevent accidental firing of a stored charge.

2. An aural and visual warning system will activate as soon as the capacitor banks have begun to charge.

3. The room will be brightly illuminated so that the pupil of the eye will be small.

4. Very high-energy lasers will be fired by remote control. An alternative would be the complete enclosure of the laser and its beam.

5. Fireproof materials such as fire brick should be used as a backstop for the beam.

6. Eye protection such as goggles of the correct attenuating optical density (OD) will be worn whenever there is a possibility of accidentally intercepting a hazardous laser beam. Table 10-32 (Ref. 9) is a guide for the selection of optical density goggles. This table lists the maximum power, or radiant exposure, for which adequate protection is afforded by filters of optical densities 1 through 7. The lenses should be curved to reduce specular reflection hazards.

7. When lasers of Classes 2, 3, and 4 are operated, the areas and equipment will be provided with warning signs and labels. Examples of such signs and labels are shown in Fig. 10-35 (Ref. 49).

The CAUTION labels (Fig. 10-35(A) and (B)) are characteristic of those found on Class 2 laser products or Class 3a visible laser products. The DANGER labels (Fig. 10-35(C) and (D)) are characteristic of those found on Class 3b and Class 4 products. The wording is in accordance with the Bureau of Radiological Health (BRH) performance standard, which requires an indication of either the laser medium or wavelength(s), the maximum output of laser radiation, the pulse duration, if appropriate, and a directional sunburst logotype. These warning labels should be prominently displayed on the laser near the operating controls to alert the operator.

Anyone who uses or maintains a laser and its equipment should first be trained to understand and become familiar with its hazards and safety procedures. If practicable, any laser used in a training or test environment should be equipped with filters or other means to attenuate its output and thereby reduce the possibility of injury. Wherever possible, specular objects that could accidentally reflect the beam should be removed from the field of fire. Targets for laser testing should be designed to absorb rather than reflect laser energy.

Whenever possible, the laser should be used in a controlled environment to preclude accidental irradiation of populated areas or personnel. Some lasers can be hazardous to human eyes over a distance extending many kilometers. Therefore, the laser firing procedures and radiating area must be controlled in accordance with the applicable safety procedures.

The optical radiation hazards to personnel and materiel have been discussed in the previous paragraphs. The equipment necessary to energize the laser presents additional hazards. The high-voltage, high-energy electrical power supplies fire the flash lamps, which in turn pump

TABLE 10-32. SIMPLIFIED METHOD FOR SELECTING LASER EYE PROTECTION FOR INTRABEAM VIEWING FOR WAVELENGTHS BETWEEN 400 AND 1400 nm (Ref. 9)

Q-Switched Lasers (1 ns to 0.1 ms)		Non-Q-Switched Lasers (0.4 ms to 10 ms)		Continuous Lasers Momentary (0.25 to 10 s)		Continuous Lasers (Long-Term Staring Greater Than 3 h)		Attenuation	
Maximum Output Energy, J	Maximum Beam Radiant Exposure, $J \cdot cm^{-2}$	Maximum Laser Output Energy, J	Maximum Beam Radiant Exposure, $J \cdot cm^{-2}$	Maximum Power Output, W	Maximum Beam Irradiance, $W \cdot cm^{-2}$	Maximum Power Output, W	Maximum Beam Irradiance, $W \cdot cm^{-2}$	Attenuation Factor	OD
1.0	2	10	20	NR	NR	NR	NR	10,000,000	7
10^{-1}	2×10^{-1}	1.0	2	NR	NR	1.0	2	1,000,000	6
10^{-2}	2×10^{-2}	10^{-1}	2×10^{-1}	NR	NR	10^{-1}	2×10^{-1}	100,000	5
10^{-3}	2×10^{-3}	10^{-2}	2×10^{-2}	10	20	10^{-2}	2×10^{-2}	10,000	4
10^{-4}	2×10^{-4}	10^{-3}	2×10^{-3}	1.0	2	10^{-3}	2×10^{-3}	1,000	3
10^{-5}	2×10^{-5}	10^{-4}	2×10^{-4}	10^{-1}	2×10^{-1}	10^{-4}	2×10^{-4}	100	2
10^{-6}	2×10^{-6}	10^{-5}	2×10^{-5}	10^{-2}	2×10^{-2}	10^{-5}	2×10^{-5}	10	1

Note:

By using this table, higher than necessary optical densities (OD) may be obtained.

NR — Not recommended as a control procedure at these levels. These levels of output power may damage or destroy the attenuating material used in the eye protection. Skin protection would also be required at these levels.
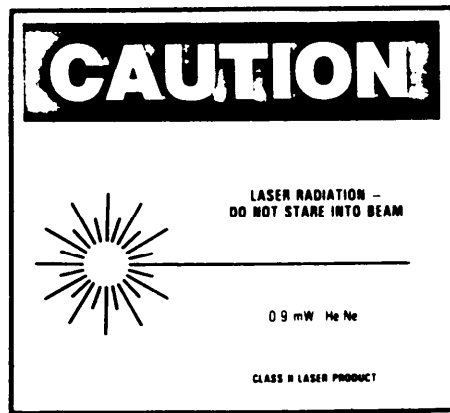
(A)
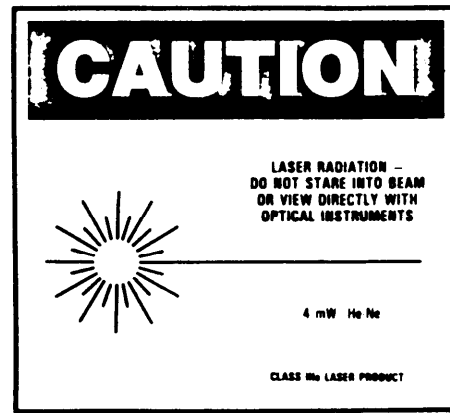
(B)

(C)
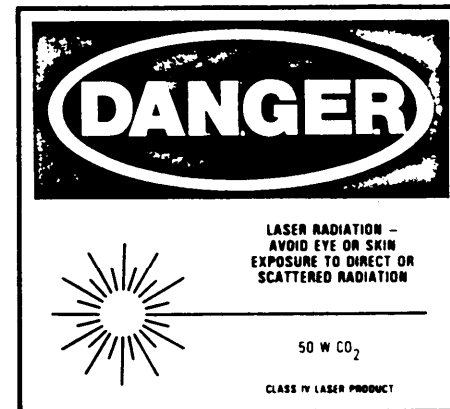
(D)

Figure 10-35. Representative Labels of the Bureau of Radiological Health (Ref. 49)

energy into the laser material. Alternatively, the power supplies power electron guns that "shoot" (accelerate) electrons to impact on the laser material. These power supplies can produce electrical shock and/or burns.

Chemical burn, toxic, and corrosion hazards are caused by the chemicals used in lasers. Vaporized targets can also produce a toxic atmosphere. Other hazards to personnel and equipment result from the possibility that the high-voltage power supply or the electron gun will generate X rays; the chance that a flash tube will explode or cause a radiation injury to the eye if tested with the cover open and, therefore, unpressurized; and hearing hazards that can be present due to electrical resonance in mechanical parts, gas discharge in chemical lasers, or pulsing of very high-energy lasers. The electrical power supplies in high-energy impulse lasers use larger capacity condensers. When charged, these devices can enable inadvertent firing even when the power supply has been turned off. In addition, these large condensers can cause formidable electrical shocks and burns. Any applicable maintenance or testing procedures must consider that

these condensers can store high-voltage electrical energy for relatively long periods (hours) and should be grounded before maintenance operations. At least four deaths have been attributed to electrical shock from laser power supplies (Ref. 49).

Laser targets for aligning, maintaining, and training should have dull surfaces, be nonreflecting, and be noncombustible at the beam intensity to avoid reflecting energy or catching fire. The laser should never be used in an environment containing flammable vapors, liquids, or other combustible materials. Table 10-33 (Ref. 46) lists some precautionary measures for laser operations.

The Army, because of the versatility and usefulness of the laser, is actively engaged in the evaluation of laser characteristics and their effects. The fact that the laser also is extremely dangerous should not be ignored in this pursuit. Accordingly, every means must be taken to provide interlocks, shields, proper training, warning devices and labels, and other safety steps to minimize the hazards and prevent accidents. Considerable laser background information of interest to the designers and

the control of a hazard has already been lost, and this makes the initial danger level much higher.

The failure of escape, survival, or rescue equipment may be worse than if that equipment had not been supplied. In some instances, the items themselves have injured the users because of their poor design or manufacture. In a crisis, failure or inadequacy of the escape, survival, or rescue equipment produces traumatic shock over and above that produced by the original mishap. In addition, the time lost in establishing that the equipment does not work or works improperly, then determining an alternative course of action, and finally taking that action under stress combine to reduce the chances of success. To make matters worse, alternative courses of action may now be impossible because the time to implement them has been lost.

The need for escape and rescue equipment and procedures must be established by contingency analysis. Once this task is done, the equipment must be selected carefully. The equipment must be analyzed to insure that it will fulfill all foreseeable needs and that procedures for its use are readily available and adequate. The equipment should be studied in detail through failure mode and effects analysis (FMEA) or other methods. A test program must be developed to insure that the items will function under expected conditions, that they will satisfy established requirements, and that procedures are adequate. Tests also should be conducted under worst-case conditions to determine whether or not the equipment can be operated and the procedures followed by a partially incapacitated person.

Sometimes escape and rescue equipment that is initially suitable for emergencies is not properly maintained. Consequently, it deteriorates and no longer functions as it should. Therefore, procedures must be established for both proper use and maintenance, and replacements must be made whenever needed.

9-2.11.1 Escape and Survival Procedures and Equipment

An example of the distinction between equipment for escape and equipment for survival is a jet pilot's emergency equipment. The ejection seat helps the pilot to escape from the aircraft; other devices enable the pilot to survive in the new environment. To survive the high-velocity air blast at ejection, the pilot must be protected by a shield or capsule. A parachute is then required so that the pilot can survive the fall to the ground. A temporary supply of oxygen and insulation against the cold may also be required. If the flight is over an ocean or lake, an inflatable life raft stocked with food and water would permit survival for an extended period. Other special provisions are required for flights over arctic, tropic, or jungle areas.

In Army tactical situations, large areas of the ground and its foliage may be contaminated with enemy chemical agents or even fallout from tactical nuclear weapons. To protect personnel from the effects of these chemicals or nuclear fallout, safety zones must be established and clearly marked. These safety zones are areas that have been decontaminated or otherwise determined to be free of hazardous materials to permit personnel to move about in these safety zones without fear of exposure. Minefields, whether prepared by friendly or enemy troops, should also be treated as "contaminated" areas requiring safety zones and routes of passage. As the tactical situation moves forward, the clear routes through contaminated areas become supply routes and evacuation routes for whatever emergencies require rearward-moving traffic.

A contingency plan identifying the most likely safety zones and evacuation routes from danger areas should be disseminated to personnel in the immediate area. The plan should be based on an analysis to determine locations where personnel will be safe or where they can withdraw during an emergency. Protective structures or routes can be provided or designated beforehand to house personnel or enable their passage to safety under certain circumstances. Contingencies to be considered are

1. The likelihood that damaging effects can occur so rapidly that reaction or escape time will be minimal

2. The damage could be so extensive that there would be difficulty evacuating the area.

3. The number of affected personnel could be so great that some would be injured in the evacuation process. (In earthquake regions a common instruction is to take refuge under a sturdy table, desk, or similar piece of equipment if the building might collapse. Similar refuges can be used if a building is damaged by an explosion and in danger of collapse.)

Escape routes should be selected and then evaluated for capacity to handle the number of personnel who would use them. Routes and exits should be marked conspicuously so that they can be followed easily. (For peacetime situations, OSHA standards require the marking of routes, egresses, and exits.) The number of exits and egresses must be adequate for the amount of escape time and number of expected evacuees in an emergency, and that number of exits must take into account the possibility that one or more of them will be blocked. Consequently, alternatives must be established. Emergency lighting may be necessary if loss of the normal lighting system could throw the routes into darkness. Egress and exit signs must be lighted, with provisions for emergency power, in buildings with numerous corridors. Emergency lighting may also be required in buildings with no natural lighting.

9-2.11.2 Rescue Procedures and Equipment

In any emergency there is the possibility that the persons involved may not be able to escape under their own resources. Accordingly, provisions must be made for rescue by other personnel should the need arise. Rescues may be attempted by

1. Persons familiar with the equipment and its operation, hazards, and emergency devices

2. Personnel familiar with the hazards in general but not with the specific equipment. For example, a city fireman may be well-trained in fire fighting but may lack training in rescuing personnel from burning aircraft.

524 (Ref. 9), AR 40-46 (Ref. 55), and in par. 6, Requirement 1, of MIL-STD-454 (Ref. 8). Limitations from Ref. 8 are quoted:

"6.1 Microwave, Radio Frequency (rf), X, and Laser Radiation Limits

"6.1.1 Applicability of Federal Standards. The design of all equipment for which a federal standard exists under the Code of Federal Regulations (CFR) Title 21, Chapter I, Subchapter J, on the Radiation Control for Health and Safety Act of 1968, shall conform to the appropriate federal standard."

"6.1.4 Laser Radiation. Laser equipment and system design, installation, and written operational and maintenance procedures shall conform to CFR, Title 21, Chapter I, Subchapter J, Part 1040. If Title 21 cannot be met because of operational requirements, an exemption shall be requested from the procuring activity and applicable military laser safety regulations shall be used as a design requirement.

"6.1.5 Radiation Level Tests. All microwave, rf, X, and laser radiation levels emanating from equipment shall be verified by documented tests to demonstrate compliance with this requirement. When modifications to the equipment affect performance or intended function, radiation levels shall be verified.".

Tolerance levels and safe limits for microwave radiation from the BRH and OSHA standards (mentioned in par. 10-8.1.7) are also given in Ref. 8. Radiation exposure limits for ionizing radiation are given in Table 10-24. ANSI Z136.1 (Ref. 56) is generally used as a guide for radiation information, although there are slight differences between the BRH and ANSI stipulations.

10-8.4 POTENTIAL HAZARD SOURCES

The only difference between X rays and gamma radiation is the source. X rays are man-made; gamma radiation results from a natural decay process. X rays can be generated inadvertently when a potential higher than 15,000 V causes electrons to strike a suitable metal surface. Army materiel in which such conditions may exist include communications and radar systems. Gamma radiation hazard may be generated by test equipment for the radiation inspection of metals and solid propellants for missiles, but such equipment is usually located at industrial facilities.

Materials that emit alpha and beta radiation are used infrequently in Army equipment. When they are used—such as in lens coatings, static eliminators, or smoke detectors—the radiation levels are too low to be injurious under any reasonable situation. The potential for harm from these radioactive materials lies in the lack of care by personnel in the machining of the material by filing,

grinding, or welding or by placing the material in contact with one's body for long periods of time.

Radar communication equipment generate microwave radiation. Infrared and ultraviolet are now both used for laser radiation of wavelengths depending on the characteristics of the radiation desired. The increasing use of lasers for range finding and as target designators could increase the hazards of eye damage unless design safeguards—such as operator filter lenses—are incorporated and suitable field procedures are used to protect friendly personnel.

10-8.5 HAZARD CONTROL TECHNIQUES

The priorities described in par. 9-1 apply equally to many radiation hazards. For example, unintended production of X rays can be eliminated by keeping electrical potentials below 10,000 V or by avoiding the use of shielding materials with a high atomic number, such as lead and tungsten, when high voltages are employed. Whenever possible, use aluminum for shields. When X rays are necessary for a specific purpose, the level of intensity and duration of exposure should be kept to a minimum. When intensity levels could be injurious, barriers and interlocks can be designed into the system (Ref. 57) and safe procedures developed for use of the X-ray equipment.

Because harmful radiation generally cannot be seen and only occasionally can be felt, personnel should not be relied upon to safeguard themselves. Unfortunately, mission requirements for the beneficial use of radiation sometimes do not permit incorporation of design safeguards that will eliminate all reliance on personnel. In such cases, warnings are necessary. For example, the Department of Defense, OSHA, Bureau of Radiological Health, and American National Standards Institute all require labeling of lasers. MIL-STD-454, Requirement 1, par. 9.2 (Ref. 8), and DARCOM-R 385-29 (Ref. 58) require that military exempt lasers be labeled to indicate such exemption. The rationale and label requirements that follow are quoted from DARCOM-R 385-29:

"The safety criteria applicable to industrial and research lasers will be applied to the extent possible to tactical laser systems designed for combat operations or combat training operations, and to laser products classified in the interest of national defense. Such devices have been exempted by the Commissioner of Food and Drugs from the provisions of Title 21, Chapter I, Subchapter J, Parts 1040.10, 1040.11, and 1002 (except 1002.20) of the Code of Federal Regulations. As a condition of this exemption, such lasers will be clearly identified either by the label set forth below, or by other means.

CAUTION

This electronic product has been exempted from FDA radiation safety performance standards prescribed in the Code of Federal Regulations, Title 21, Chapter I, Subchapter J, pursuant to Exemption No. 76EL-01DOD issued on July 26, 1976. This product should not be used without adequate protective devices or procedures.

"When a laser is to be identified by means other than the above label, the proponent...[AMC] element will submit detailed information as to the alternative means of identification and the justification for such means through the Director,...[AMC] Field Safety Activity, ATTN: DRXOS-ES, Charlestown, IN 47111, to the Commander,...[AMC], ATTN: DRCSF-P, 5001 Eisenhower Avenue, Alexandria, VA 22333.".

Additionally, Army systems operating at 10 MHz or above and lasers and other high-intensity light sources must be reviewed and approved by the US Army Environmental Hygiene Agency (USAEHA) for safe design and operating procedures. In addition, Ref. 8 (par. 9.2) requires that any item that can emit hazardous radiation be labeled.

Furthermore, personnel areas that may receive harmful radiation should be posted with warning signs and controlled to prevent entry of persons when equipment is radiating. Although this requirement primarily affects persons in charge of operations, the operators must be provided with information describing the limits of the hazardous areas. In addition, designers may be required to incorporate interlocked warning lights or audio signals to warn personnel that equipment is generating hazardous radiation. One type of safety interlock to prevent inadvertent operation of radiating devices is reproduced here as Fig. 10-36 (Ref. 57). The same type of logic functions can be designed for any electrically controlled equipment to prevent an inadvertent hazardous operation.

10-8.6 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

The following guidelines should be followed to protect against radiation hazards:

1. When radiation-type hazards are identified at the beginning of a program, determine which sources can be eliminated or reduced in degree of hazard potential consistent with the military performance requirement and/or by an alternative design solution.

2. Insure that for all electrically initiated radiation devices, the senior operator's or commander's control station is equipped with positive means to control the output radiation—e.g., on/off, low/high energy—and the various radiation characteristics—e.g., frequency and scan. In some designs, as for Class 3b and Class 4 lasers, the control station must be equipped with a key lock unless an exemption for reasons of military necessity is approved by the Army command responsible for the development of the equipment.

3. Insure that ionizing radiation radioisotopes are identified, labeled as in Fig. 10-37, stored, installed in equipment, operated, and disposed of in accordance with Nuclear Regulatory Commission (NRC) regulations (10 CFR 19 and 20), Limitations of the National Council on Radiation Protection; and AR 385-11 (Ref. 54).
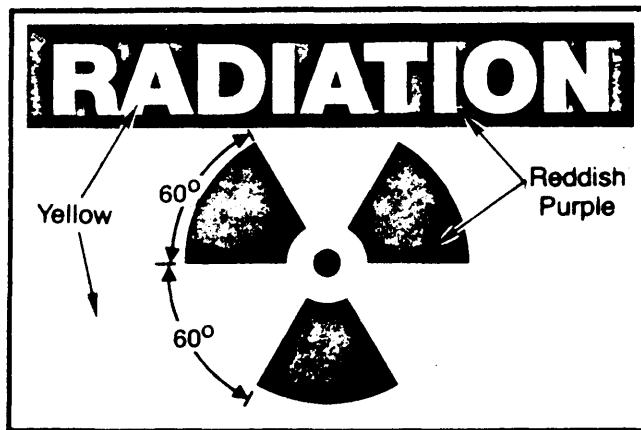
Figure 10-37. Radiation Label

4. Provide passive warning signs and active warning devices—both aural and visual—that operate when equipment is radiating unless exempted for reasons of military necessity by the Army command that has development responsibility for the equipment.

5. Provide remote control capability for activating extremely hazardous radiation devices such as very high-energy lasers and for the removal of transportation shielding from radioisotopes whose radiation exceeds safe exposure limits for personnel. Generate countdown procedures that will be compatible with remote control capabilities.

6. Use design techniques and materials that will be compatible with the entire scope of the equipment life cycle including each operating, testing, and repairing environment for each part of the equipment. In addition to the primary Army combat mission and its scenario, consider also the peacetime environments of operation and training:

   a. Do not use flammable materials or materials that can become radioactive through bombardment by high-energy particles.

   b. Design safety features for durability so they will remain effective through many cycles of operation in training, testing, and repairing.
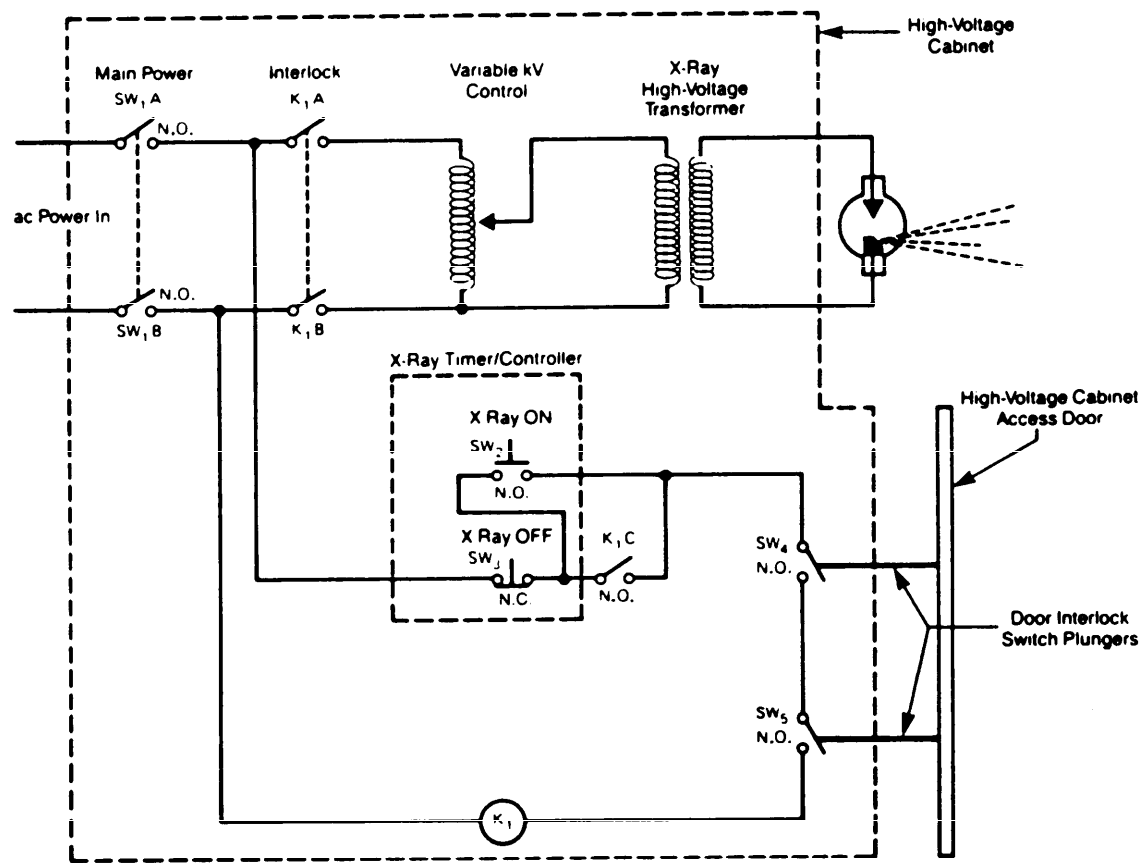
(A) Electrical Power Interlock Circuit
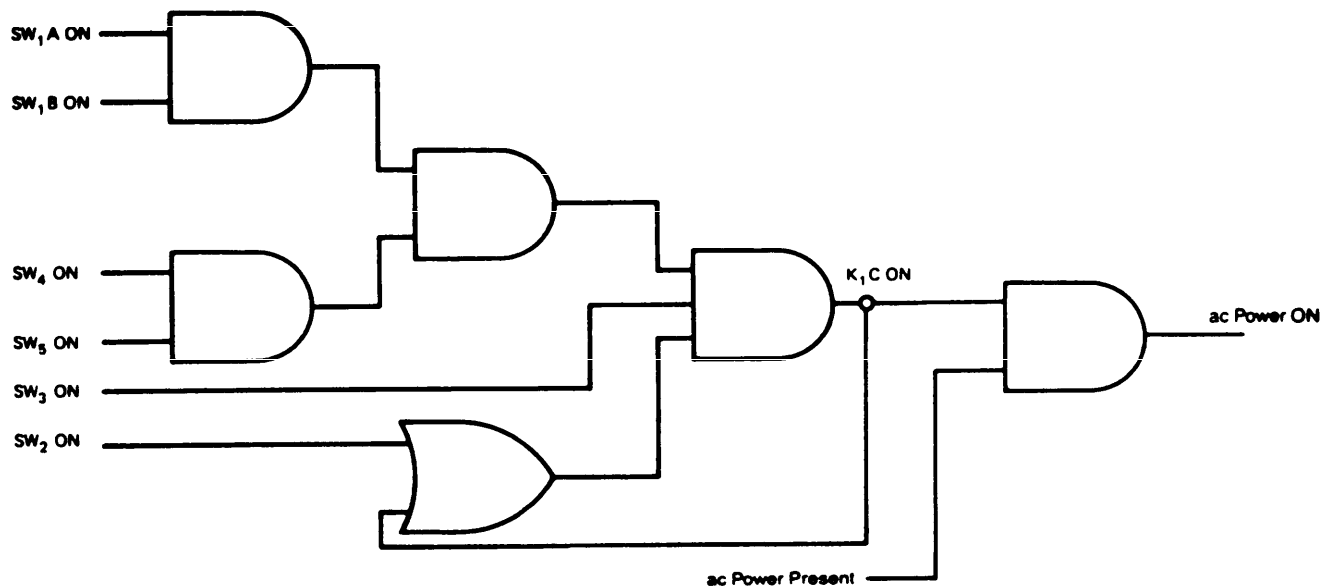
(B) Equivalent Interlock Logic Diagram

Figure 10-36.   X-Ray Safety Interlock Circuit (Ref. 57)

c. Equip optical radiators with automatic filters for eye protection to reduce the dependence on actions of operators for self-protection.

d. Where there is a reasonable possibility of inadvertent radiation in personnel areas, provide active radiation detection and alerting devices.

e. Placard laser devices, microwave emitters, and sources of X rays and radioisotopes with the characteristics of the type of radiation emitted so that protective goggles, clothing, and other protective equipment can be properly chosen.

10-9 CHEMICAL REACTIONS
10-9.1 GENERAL

Chemical reactions can be extremely violent; consequently, they can cause immediate, severe injury through explosions, dispersion of hazardous materials, and creation and emission of large quantities of heat. Other chemical reactions may be slow and very mild, and their effects may become apparent only over long periods of time. These gradual effects can contribute to failures of equipment or structures, which can then cause injuries or damage.

The quantity of energy required to initiate a reaction under specified conditions depends on the substance(s) involved, but for any specific substance the quantity always remains the same. The initiation energy will consist of the heat already contained in the substance(s), as indicated by the temperature(s), plus any input energy. If the temperature of the substance(s) is high enough, the reaction will initiate spontaneously. In addition, reaction rates will increase with an increase of temperature of the reactant(s) (Le Chatelier's principle).

Several types of chemical reactions are of interest to system safety engineers:

1. *Dissociation*. A reaction in which there is a breakdown of a molecule, either simple or complex. In all reactions, however, the first step is dissociation.

2. *Combination*. A reaction in which various reactants combine to produce stable molecules

3. *Corrosion*. A reaction that is a slow combination process

4. *Replacement*. A reaction in which a very active chemical radical replaces a less active one in a molecule. Each of these reactions is discussed in subsequent paragraphs.

Reactions can also be classed as exothermic, heat producing, or endothermic, heat absorbing. Each reaction may be a complex process with many steps which may be exothermic or endothermic. The net thermal end result of the complete reaction is the sum of the heat gains and losses of each of the intermediate steps.

Each of these types of chemical reactions could occur in various Army systems. They may or may not be desirable, depending on the principles of operation of the system,

the environment in which the system is operated, and other constraints or requirements imposed on the system. The discussion of each of these chemical reactions includes information about the sources of the hazards, techniques to control the hazards, and safety criteria for designers to follow. In most of the reactions discussed, there is no safe limit for personnel or equipment. If the reaction takes place, the result is generally either a life-threatening or equipment-damaging situation.

10-9.2 DISSOCIATION REACTIONS

Dissociation is the breakdown of the molecule of a chemical compound. Depending upon the circumstances, dissociation of a molecule can release tremendous amounts of energy very quickly. High-explosive molecules dissociate in exothermic reactions, which release great quantities of heat and gas after the threshold level of energy has been applied to initiate the reaction. The threshold necessary for dissociation varies with each compound and depends upon its chemical stability. For example, to avoid inadvertent activation, high explosives for Army use generally are very stable and require activation by small amounts of sensitive initiating explosives. Another example is trichloroethylene, a solvent that was widely used until it was found to be a carcinogen. This is highly stable chemically but will dissociate violently when subjected to high initiating energy such as that from a welding torch or an explosion.

Classes of chemicals that will dissociate violently (and quickly) include chlorites and chlorates, nitrates and nitrites, permanganates and chromates, and iodates and bromates. Most of these items are strong oxidants and, in contact with organic matter, can cause explosions and fire. The reactions of these compounds are exothermic; the material decomposes rapidly, which liberates oxygen or oxidizing radicals that react with other radicals to form stable compounds.

Peroxides make up some of the most highly sensitive materials. Peroxides are used for cleaning because they are powerful oxidizers, but this same property makes them hazardous except under cool, quiescent conditions. Powerful concentrations of barium peroxide, sodium peroxide, hydrogen peroxide, and other peroxides can cause fires and explosions when heated or moistened while in contact with combustible material. Most hazards with peroxides can be avoided by use of oxidation inhibitors or by careful temperature control. There are other extremely sensitive materials as indicated in the next paragraph.

Acetylene (C_4H_4) is extremely sensitive at pressures over 103 kPa (15 psi). It will dissociate

$$C_4H_4 \rightarrow 2C_2 + 2H_2 + \text{energy}$$
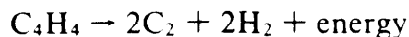
if shocked mechanically and can explode violently.

Liquid ozone (O_3) is so extremely unstable

$$2O_3 \rightarrow 3O_2 + energy$$
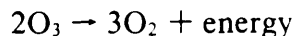
and sensitive that it can detonate from the shock of being poured from one container to another. Liquid oxygen in contact with organic materials will cause them to become unstable and sensitive and thus create explosive mixtures.

10-9.3 COMBINATION REACTIONS

A combination reaction is one that results in reactive particles combining to form stable molecules. These reactions may also release energy. Fires occur when fuel and oxidizer molecules break down into reactive particles after initiating energy has been applied and then unite into new combinations in a self-sustaining process. Fire is a complex mixture of dissociation and combination processes that absorb and release energy, but the net balance is one in which thermal energy is released. Anything that will enhance these individual reactions, such as a catalyst, will make the overall reaction progress faster. Anything that will interfere with these individual reactions—such as the presence of nonreactive particles that prevent active ions from striking each other or a reduction in temperature, which slows the motions of the ions and the breakdown of unstable molecules—will slow and perhaps stop the reaction.

Some chemicals interfere with and slow down the overall rate of the chemical reaction. This fact can be used to inhibit undesirable combination reactions such as an accidental fire. Carbon dioxide interferes with chain reactions involving hydrocarbons—which is why it is used in fire extinguishers—by producing ions that combine with the usual particles involved and prevent the reaction from proceeding to its usual end. Nitrogen will not usually interfere chemically but, as a diluent, will interfere with physical contact between the particles. Therefore, although both carbon dioxide and nitrogen are normally inert gases and will stop a fire by dilution, carbon dioxide is more effective as an extinguishant because of its interference with the intermediate chemical reactions.

10-9.4 CORROSION

Corrosion is a highly significant problem in Army systems principally because of the losses of functions which can result from metal failures and the potential for causing accidents that result in personal injury. Consequently, corrosion may present a safety problem. Corrosion is a slow combination process that affects metals and in which the reaction is slow and heat is released very gradually. Corrosion leads to loss of strength, integrity of the metal affected, and possible loss of electrical conductivity. In a pressure vessel, it may

cause rupture or a leak; in mechanical parts, it causes roughness of surfaces, contamination of products, and binding of moving parts (Ref. 59). Exposure of susceptible metals to moist air usually results in corrosion. Leaking or spilling of reactive substances onto metals will also result in corrosion, as will electrolytic action between two metals in contact.

Corrosion is generally an electrochemical process, but it can also be caused by mechanical factors such as the conditions that lead to the destruction, or simple removal, of protective scale on turbine engine blades or the abrasion of protective coatings. The rate, type, and extent of corrosion will depend on a variety of environmental conditions. It is a surface phenomenon that begins and continues where the unaffected metal is exposed to the environment and continues into the base metal as new surfaces are exposed.

Galvanic action (electrolytic) corrosion occurs between two metals in an electrolyte that create an electrochemical cell. The two metals do not necessarily have to consist of different materials or even be separate pieces. The galvanic action can occur in the surface of a single piece containing inhomogeneities in composition or physical structure (Ref. 60). The metals form the anode and cathode of the cell in which reactions take place. Moisture, nonpure water, generally acts as the electrolyte. Pure water is not an electrolyte, and metals will not corrode in pure water. Unfortunately, the presence of even a small amount of foreign matter can make water an active electrolyte.

In general, the tendencies for metals to corrode depend on their relationships in the electromotive force (EMF) series. Some metals, pure gold and platinum—"noble" metals at the cathodic end—will not corrode. Metals at the anodic end of the EMF series have high corrosion tendencies. The relative positions of some metals in the series are given in Table 10-34 (Ref. 60).

The rate of reaction between two metals is also governed by how far apart they are located in the electromotive series. Metals forming an electrolytic cell spaced far apart will experience intense galvanic action. The types of corrosion that result will depend on the metal undergoing corrosion. The rust resulting from corrosion of iron can occur in a number of ways and forms a porous oxide that leads to further corrosion. On the other hand, aluminum generally corrodes in a uniform manner over its surface to produce an oxide that usually provides an overlying layer of protection for the metal beneath. Although there has been no general consensus on the types of corrosion possible, it has become convenient to group the various corrosion phenomena into nine forms of corrosion. These groups contain overlapping or similar characteristics as well as distinct differences in the processes. The types of corrosion are grouped as follows:

1. *Uniform Corrosion.* Occurs over the entire surface

TABLE 10-34. THE GALVANIC SERIES OF METALS AND ALLOYS (Ref. 60)

Anodic End	Magnesium
	Magnesium Alloys
	Zinc
	Galvanized Steel
	Aluminum 1100
	Aluminum 6053
	Alclad
	Cadmium
	Aluminum 2024
	(4.5 Cu-1.5 Mg-0.6 Mn)
	Mild Steel
	Wrought Iron
	Cast Iron
	13% Chromium Stainless Steel
	Type 410 (Active)
	18-8 Stainless Steel Type 304
	(Active)
	18-12-3 Stainless Steel Type 316
	(Active)
	Lead-Tin Solders
	Lead
	Tin
	Muntz Metal
	Manganese Bronze
	Naval Brass
	Nickel (Active)
	76 Ni-16 Cr-7 Fe Alloy (Active)
	60 Ni-30 Mo-6 Fe-1 Mn
	Yellow Brass
	Admiralty Brass
	Aluminum Brass
	Red Brass
	Copper
	Silicon Bronze
	70:30 Cupro Nickel
	G-Bronze
	M-Bronze
	Silver Solder
	Nickel (Passive)
	76 Ni-16 Cr-7 Fe Alloy (Passive)
	67 Ni-33 Cu Alloy (Monel)
	13% Chromium Stainless Steel
	Type 410 (Passive)
	Titanium
	18-8 Stainless Steel Type 304
	(Passive)
	18-12-3 Stainless Steel Type 316
	(Passive)
	Silver
	Graphite
	Gold
Cathodic End	Platinum

From *Corrosion Engineering* by M. G. Fontana and N. D. Greene, McGraw-Hill Book Company, New York, NY, 1967.

at the same rate. This is the most prevalent form of corrosion; it generally extends over the entire exposed surface or large parts of the exposed surface.

2. *Galvanic Corrosion.* Occurs in a cell where two metals and an electrolyte are localized. This can occur on a macro scale where two parts of different metals are joined or on a micro scale where the different materials are in the surface of one part.

3. *Intergranular Corrosion.* Occurs in boundaries between grains and crystals of the metal. Boundary areas are usually anodic to the grains, often due to impurities in the metal. This type of corrosion is generally not significant, but in special cases it is very serious when exfoliation, i.e., scaling, can occur.

4. *Pitting Corrosion.* Very localized but often widespread in occurrence. Pitting is usually initiated at highly anodic points in the surface of the metal. These points may be due to differences in chemical composition, coating irregularities, worked regions, surface scratches, and emerging dislocations.

5. *Crevice Corrosion.* Very similar to pitting corrosion. Metal susceptible to pitting will also be susceptible to crevice corrosion, but the converse is not true. This process is characterized by intense localized attack in crevices such as at lap joints, under bolt and rivet heads, and at holes or locations of surface deposit (of foreign material).

6. *Erosion-Corrosion.* Occurs when corrosion products are removed and new metal surfaces are subject to attack. It occurs when particles in a liquid impinge on a metal surface and erode the protective films. Fretting corrosion is an erosion action resulting from mechanical surface movements under pressure.

7. *Stress Corrosion.* Results from corrosion on metals under stress; the result is cracking. When the stress is cyclical, it is referred to as "fatigue corrosion". Ordinarily, however, the stress is nonfluctuating, in which case there must be at least a tensile component of stress.

8. *Selective Leaching.* Selective removal of a single element from an alloyed metal by corrosion processes. Examples of this corrosion are the removal of zinc from brasses and the removal of aluminum, chromium, cobalt, iron, and some other metals from various alloys.

9. *Hydrogen Stress Cracking.* Due to the combination of absorption of hydrogen by the metal and stress of the part. A good example of this process is the sudden catastrophic failure of highly stressed landing gear parts on aircraft parked on a ramp. The principal reason for failure is that the parts were not processed to remove the source of hydrogen during manufacture.

The usual protection against corrosion is by specifying a metal that will be compatible with the substances it will contact or by providing the metal with a protective covering such as paint or plastic. Other methods of protection are the removal of moisture or foreign material

from contact with the metal surface or use of an inert gas to provide a surface film that acts as a barrier.

The adverse effects of the hazards of corrosion are all related to reducing the amount of "solid" load-carrying material from parts or initiating weakness through other processes, which result in cracks and failures under stress. Crevice corrosion in electrical equipment can also lead to increases in circuit resistance. If not found and corrected, these points of increased resistance form localized "heaters" when carrying current. The heat of these resistance points can damage other electrical components or, in extreme cases, cause an electrical fire.

Uniform corrosion will continue to make metal parts thinner, and if the designer does not compensate for this effect, the part will eventually fail in service. Through testing, the life of a part can be predicted if this type of corrosion is a factor.

Other localized types of corrosion—such as pitting, crevice, stress, and galvanic (localized form)—cause safety problems of various types. The exact type of safety problem depends on the equipment, the manner in which corrosion was considered, and the solutions implemented during its design. The failure of parts under stress has been mentioned. In addition, pressure vessels may leak due to pitting, surfaces meant to be smooth become roughened and can cause binding, and parts that must be disassembled may be "bonded" by corrosion.

10-9.5 REPLACEMENT REACTIONS

Replacement is the type of reaction in which a highly active chemical radical takes the place of a less active one in a molecule. For example, fluorine, being more active than oxygen, will replace oxygen in water to form hydrogen fluoride. Replacement reactions of this type are rare in Army systems. Occasionally, double replacements may take place in which two more stable compounds are formed. For example, sodium hydroxide will react with ammonium chloride to give the more stable compounds sodium chloride and ammonium hydroxide. Hazards can result from mixing compounds that react by means of double replacement to form an extremely dangerous product. For example, mixing sodium hypochlorite (in some bleaches) with an acid releases chlorine gas, which can be lethal, especially in an enclosed space. Accordingly, each time different chemical compounds are to be mixed or stored together in close proximity, all possible chemical reactions should be investigated to insure that

    1. No hazardous reactions will take place.

    2. No hazardous products will be created.

Ref. 41 provides guidance for avoidance of incompatible material situations, i.e., lists compounds that are incompatible with each other.

10-10 CONTAMINATION

Contamination can be defined as the presence of any undesired gas, liquid, or particulate matter in a desirable material or in a specific environment such that injury, damage, or loss of function can occur. Contamination can arise from various sources such as the environment itself, chemical reactions, the actions of personnel, production processes, and other materials extraneous and foreign to the desired substance. It can take the form of solids, liquids, or gases and can appear as solids, liquids, or gases in any combination.

In any chemical reaction, the temperature of the reaction will affect the rate of reaction—higher temperatures cause faster reaction rates. A contaminant may interfere with the temperature of a reaction and cause an abnormal reaction rate that may make the reaction unstable and dangerous. Some contaminants may even act as catalysts to cause the initiation of unwanted reactions. For example, even a small amount of copper present as a contaminant will initiate the dissociation of hydrazine.

Numerous unexpected hazards—such as malfunctions, chemical reactions, or injury—can be caused by contamination. Contamination can clog passages and cause higher pressures in lines and thus increase the possibility of line or vessel rupture. The blockage of lines could also prevent lubricants, fuels, or coolants from reaching downstream units where they are required for the continued safe operation of the system.

Contamination can clog valves, filters, nozzles, regulators, and orifices. It can score and wear lines by means of friction abrasion. Thus contamination can increase pressures in systems and cause damage, including violent ruptures, sometimes resulting in the spillage of potentially hazardous material over a large area or on personnel and equipment.

Contaminants can increase friction in moving parts, resulting in increased wear, equipment overheating, and possibly a fire. Contaminants can induce corrosion and, in some instances, the generation of static electricity in tanks containing petroleum products. In chemical reactions, such as in internal combustion processes, contamination can cause uneven burning or reduced or increased burning rates. Contamination in turbochargers can also cause uneven burning, wear of turbine blades, or friction problems.

There are a number of methods of preventing contamination; to select the appropriate one, the analyst must first identify how the contamination could occur initially. Contamination can result from external entry of an unclean environment, from spillage or leakage, chemical reactions (primarily corrosion), or failures of filtering

equipment. The best prevention is to insure clean equipment, adequate filters and filtering processes and procedures, and to prevent spills and leakages by means incorporated during the design process.

Contamination can also occur from internal processes in a completely closed system. The contamination can be generated inside by polymerization, breakdown of chemicals such as polymers, microbial or fungal growth (biological agents), wear from metal surfaces in moving contact, or chemical reactions between a fluid and the material in its container. Prevention of these types of contamination can only be accomplished during the design process.

10-11 MATERIAL DETERIORATION

Material deterioration is the weakening or failure or change of a material. This weakness or failure can cause hazardous situations of importance to the designer. There are many causes of deterioration—e.g., corrosion, constant stress, vibration, aging, wear, heat from friction, moisture, radiation environment, and even insects.

Corrosion can be caused by oxidation (rusting), whereby the metal is slowly converted to substances that do not have the strength required in the design. It can be caused by electrolysis, during which galvanic action slowly eats the metal away. See par. 10-9 for a further discussion of these reactions.

Constant stress can change the characteristics of a material. Where a steel bolt is constantly stressed near its elastic limit, it can gradually elongate and finally fail. If the part is critical, an accident could result. The designer, therefore, must use a safety factor to insure the material can withstand anticipated deterioration during its expected useful life and still meet design strength requirements.

Vibration of material can cause a constant flexing, and over a period of time this flexing can weaken a section; the material may break and create a potentially hazardous situation. The designer must assure that vibration of critical components and parts is controlled to safe limits through the use of shock mounts or substantial hard mounts. Critical mechanical alignments also can be lost because of vibration. Care must be taken to identify vibration-susceptible parts—from a safety-critical and damage mode standpoint—and to establish test procedures that will verify the input vibrations and the vibration-controlling design feature.

Some materials grow old, just like humans, in the environments of the real world; consequently, the characteristics of the material change with time. Polymers and other nonmetallic materials can shrink and crack, and aluminum under compression can change shape. Though it may be debatable whether age alone causes materials to change, the reality is that materials, while aging, are also constantly subjected to some type of environment. Natu-

ral environments of solar radiation, humidity, atmospheric pressures, contamination, and wind—each with daily variations—contribute to material degradation. Electrical potting and insulating materials are common examples of materials that are susceptible to deterioration with age. Potential hazards develop when these materials are used in high-voltage equipment or where short circuits can result in large flows of electric current. In signal circuits the deteriorated insulating material will admit moisture; this can combine with impurities present to create unwanted signal paths, a hazard. To avoid this problem, preventive maintenance procedures are established for the purpose of replacing aging materials before they fail. In these cases the designer must assure that the life expectancy of various parts is based upon data on properties of materials that take into account aging in the expected environment. Timed replacements—hours of service, rounds fired, etc.—must then be established for safety-critical parts to prevent a hazardous situation from developing as materials deteriorate.

When two materials rub against each other, wear occurs. One or both of the materials is gradually worn away until the design parameters are no longer being met. In a critical area this can create a hazardous condition. The designer must assure that stresses and corresponding wear are determined early in the system acquisition program to forecast accurately the life expectancy of safety-critical components. In a similar fashion, when two materials rub against each other, the friction will generate heat that can cause deterioration of the material. In the case of steel parts that require specialized heat treatment for sufficient strength, the friction heat generated by rubbing can reduce the strength and allow a failure. Testing to destruction can often identify such areas.

Moisture is responsible for other types of deterioration. There are numerous chemicals that will not react with other materials when dry, but in contact with moisture or water a chemical reaction begins and the materials undergo a chemical change. Accumulation of condensed moisture or water from leaks can cause leaching of soluble portions of mixtures whose properties will then be altered. If the material is wood and and it is attacked by fungi, dry rot will occur and the wood will lose its structural strength. This can be hazardous, particularly where wood crates and pallets are used. A very good design technique to keep moisture out of cavities where it can damage materials is to provide drain holes for the accumulated moisture to run out. Seldom can one expect to keep all forms of moisture from entering equipment, but the equipment can be kept reasonably dry by providing an exit for the moisture.

Radiation is a cause of material deterioration. Solar, ultraviolet, and infrared radiation cause a breakdown of polymers, and other synthetic materials, by initiating a chemical reaction in which hydrogen chloride (hydrochlo-

ric acid) is produced. The hydrochloric acid then further reacts with the material and breaks it down. In rubber materials, such as those used for tires, the weakening may permit the tire to rupture. The deterioration of certain rubbers is accelerated by ozone; accordingly, an ozone inhibitor must be included in their formulation for improved performance. In insulating materials, the protective value of the insulation will be lost. To protect such materials against radiation deterioration, the surfaces can be painted; the material can be combined with radiation-resistant dyes; or the materials to be protected can be covered or enclosed.

Other natural and man-made environments can hasten material deterioration and must be examined from a safety viewpoint. Extremes of heat and cold in desert or arctic climates will affect the properties of materials and can permanently alter their characteristics. Smog can hasten the deterioration of rubber products. Salt air hastens corrosion, and salt water literally dissolves some metals.

The design engineer must analyze the effects of the environment on the critical areas of the system being examined. For example, if dissimilar materials are required to insure a tight fit, materials should be chosen with low or similar coefficients of expansion. If the reaction of the equipment to extremes of temperature is critical, temperature-compensating devices may be necessary. Paints or surface treatments may protect parts from corrosion. Special rubber paints or rubber formulations, resistant to specific expected environments, should be used to control deterioration of rubber parts. If these protective design features cannot be provided, the sensitive parts should be protected by placement in enclosures (such as hangars or garages) or covered with canvas or another protective material. If the component is especially critical, it may require hermetic sealing in an inert atmosphere.

The effects of insects, gnawing rodents, birds, and other forms of animal life on the material must be considered. Termites can weaken a wooden structure much like corrosion weakens metal structures. Rats gnawing on various ordnance devices or materials can expose sensitive materials, e.g., phosphorus, to air or break off pieces of explosive—either of which may cause a fire or explosion. Birds build nests in air-cooling intakes of vehicles. When encountered by Army aircraft in flight, birds can break windows or damage structures or moving parts such as rotor blades or engines. Insects may invade sensitive equipment by building nests of mud or plug tiny holes like static air vents in aircraft.

The designer has many choices to nullify the adverse influence of animal life on Army equipment. Containers for material in storage, or otherwise unattended, can be made sufficiently strong or of repellent materials to discourage rats and other gnawing creatures. Screens can

be placed over inlets subject to clogging by insects, and covers, to be used when the equipment is inactive, can be designed for large inlets. Preoperation inspections to insure that protective measures have been effective should be a part of the designer-influenced requirements for correct operating procedure.

10-12 FIRE

Fire is a hazard that can have more varied and serious adverse effects than any other hazard if it occurs inadvertently or if loss of control occurs when a fire is being used beneficially. Although fire is a common occurrence in both its beneficial and destructive aspects, the net overall thermal result of a fire is always an output of heat. The great amount of heat released by a fire presents a serious hazard to personnel and materiel. Fire can be fatal to personnel by the inhalation of hot gases and / or smoke or burning. Materiel can be destroyed completely either by the high heat or by actual combustion in the fire.

Because it is important to know about causes and effects of fires in Army systems, designers and system safety engineers must be knowledgeable in this area. Within the past 20 yr, there has been much investigative work on fires; their initiation, reactions, prevention, and suppression have been examined. Special emphasis has been placed on the new types of fuels and oxidizers for space systems that operate under weightless conditions and aircraft operating in oxygen atmospheres. Much of this information, primarily that derived from studies for aircraft systems, is applicable to many Army systems. For example, it was learned that the use of plastic foam in a fuel tank is one of the major safety design features that makes Army helicopters safer in situations when a fuel tank is ruptured. This foam fills the tanks but occupies only about 3-4% of the volume of the tank. The fuel is partially "held" in the cells of the foam, which prevents a splash of fuel when the tank is ruptured. In normal operation, however, the fuel drains to the outlet ports at rates sufficient to operate the vehicle. Another safety feature for aircraft is a built-in fire and/or explosion detection and suppressant system that will operate so fast that the fastest burning will be damped before it reaches the catastrophic level of pressure. For additional background and detailed information on the subject, an excellent source is Ref. 50.

In accidental fires, especially in structures, the majority of deaths that occur are not due to the high temperatures and burns but to the toxic products produced. Some of these toxic products include, but are not limited to,

1. *Carbon Monoxide (CO)*. The commonest killer when fire occurs. It quickly and invisibly reaches lethal concentrations—1.28% by volume of carbon monoxide in air is fatal in 1-3 min; 0.64%, in 10-15 min; 0.32%, in 30-60 min; and even 0.16%, within 2 h. Any concentration over 0.05% is considered dangerous. The effects of carbon

monoxide are cumulative and repeated exposure at very low levels can result in lethal accumulations in the blood. Even very low levels will create dangerous situations in which operators of Army vehicles may be physically and mentally impaired due to carbon monoxide leaks in exhaust systems.

2. *Carbon Dioxide (CO₂)*. Always present when there is a fire involving an organic substance. It will replace oxygen in the air so that a breathable atmosphere no longer exists. Respiratory collapse or asphyxiation can occur when concentrations of carbon dioxide in air exceed 5.0% by volume.

3. *Hydrogen Cyanide (HCN)*. More toxic than carbon monoxide. Because it is lighter than air, it is a more dangerous hazard in enclosed spaces than in open locations. A concentration of 100 parts per million (ppm) (0.01%) may be fatal in 30-60 min. HCN is produced by combustion of chlorinated hydrocarbons, plastics, leather, rubber, silk, wool, and wood.

4. *Hydrogen Chloride (HCl)*. Produced during combustion of materials containing chlorine. It is not as toxic as hydrogen cyanide or phosgene but is dangerous during prolonged exposure because it is a strong acid, i.e., it will attack the upper respiratory system.

5. *Hydrogen Sulfide (H₂S)*. Results from incomplete combustion of substances containing sulfur, such as natural rubber, wool, hair, leather, and wood. Hydrogen sulfide is flammable and, like carbon monoxide, will burn when exposed to oxygen. Hydrogen sulfide rarely will be found in explosive concentrations. It is characterized by its "rotten egg" odor. Its presence, however, rapidly desensitizes the olfactory organs so that odor will no longer serve as a warning sign. Concentrations of 400-700 ppm (0.04-0.07%) may be fatal in 30-60 min.

6. *Phosgene (COCl₂)*. Produced during decomposition or combustion of chlorinated hydrocarbons, including carbon tetrachloride, ethylene dichloride, and hydrofluorocarbon compounds F11 and F22 (products with the Freon trade name). Toxic in extremely small dosages, phosgene at 25 ppm (0.0025%) can be fatal in 30-60 min. During World War I phosgene was used in chemical warfare.

7. *Particulate Matter*. Although very toxic gases are produced in fires, none are as injurious as the fire particles that can be inhaled. These particles consist of hot soot or ash. Soot is finely divided, incompletely burned solid matter; ash is burned material. Not only can the fire particles block the breathing passages but, because they are generally at high temperatures, can cause severe internal burns.

10-12.1 FUELS

Fuels are substances that act as reducing agents, giving up electrons to an oxidizer, by chemical combination. Fuels include elements such as carbon, hydrogen, or magnesium. They also can be single compounds such as CO or methane (CH₄), or complex compounds such as wood or rubber. Obviously fuels are numerous and varied; those which may be found in Army systems include, but are not limited to, the following:

1. Fuels for operation of internal combustion engines, heating, and welding
2. Solvents and cleaning agents
3. Wood and wood products, including paper
4. Lubricants
5. Furnishings and upholstery
6. Cloth and clothing and other flammable fiber materials
7. Flammable refuse and trash
8. Organic materials of all kinds, including rubber and plastics
9. Common hydraulic fluid (MIL-H-5606 (Ref. 61)) and some coolant fluids (Note: MIL-H-83282 (Ref. 62) hydraulic fluid has flash and fire temperature points twice as high as those of the MIL-H-5606 fluid.)
10. Normally, low-combustion materials in the presence of strong oxidizers at high temperatures
11. Hydrogen from charging batteries
12. Products resulting from incomplete combustion of organic materials
13. Paints, lacquer, or waxes used as coatings
14. Refrigerants, including ammonia and methyl chloride.

10-12.2 OXIDIZERS

Oxidizers are receivers of ions, acquiring electrons from the fuel (reducing agent), in the chemical exchange of active combustion. The atmosphere contains 21% oxygen, and this oxygen is the most common oxidizer. Oxidizer-rich environments—environments that contain an oxidizer stronger than air—permit many substances to burn that would normally be considered nonflammable or of very low combustibility. Flare-type combustion is the burning of a fuel in oxidizer-rich atmospheres, which produce a higher temperature and a more rapid rate of combustion than would be possible in a fuel-air mixture. Oxidizers include

1. Elements such as fluorine, oxygen, or chlorine
2. Compounds that will readily release fluorine, oxygen, chlorine, or other elemental oxidizers. These compounds include hydrogen peroxide (H_2O_2), potassium hypochlorite ($KClO_3$), and lead dioxide (PbO_2).
3. Other oxidizers such as strong acids—e.g., nitric acid (HNO_3), hydrofluoric acid (HF), and sulfuric acid (H_2SO_4)—and compounds such as sodium nitrate ($NaNO_3$) and nitrogen tetroxide (N_2O_4) that will release negative radicals.

Many processes employ or produce oxidizers more hazardous than air. Pure oxygen is a far stronger oxidizer than air because the oxygen in air is diluted by the

presence of nitrogen. Other oxidizers include chlorine and other halogens; nitrates, nitrites, and peroxides; and compounds such as nitrogen tetroxide. Elements considered fuels in most circumstances may be oxidizers in other instances and vice versa. For example, sulfur will burn in the presence of oxygen to form sulfur dioxide (SO_2), but hydrogen will burn with sulfur to form hydrogen sulfide (H_2S). Hydrogen sulfide is a fuel that will burn in air.

10-12.3 FLAMMABLE MIXTURES

Not only must a fuel and an oxidizer be present before a fire can occur, but they must be present in a flammable mixture. When too much fuel is present, the mixture will be "too rich"; with too little fuel, the mixture is "too lean". In neither case will it burn. The percentages by volume of fuel in air at which a mixture is too lean or too rich are the flammability limits, and the difference between the two is the flammability range.

Normally, the values of the lower flammability limit (LFL) and the upper flammability limit (UFL) are determined by tests performed under standard conditions of temperature and pressure. Table 10-35 (Ref. 63) lists the flammability limits of common substances. Ref. 63 also provides additional background on flammability limits. Whether a mixture will ignite, however, depends not only on the actual percentage of gaseous fuel in the mixture but also on such factors as the thermal energy in the ignition source; the temperature of the mixture; and the type, shape, material, and reflectivity of the container.

Both the fuel and oxidizer must be present as gases to create a flammable mixture; therefore, a suitable amount of flammable gas in air is ready for combustion. A liquid must change to a gas to create a flammable mixture, and the measure of its tendency to vaporize is also indicative of how great a fire hazard it represents. The vapor pressure of a gas is governed by the temperature required to maintain it in its liquid state. Every liquid is typified by a definite temperature at which it will provide enough gas to create a flammable mixture. If an outside ignition source is applied to the vapor above a liquid, the vapors may flame but not sustain continuous combustion. The reaction stops because the vapor pressure at this temperature is inadequate to produce enough gas to sustain continuous burning. The temperature at which this transitory flammability occurs is referred to as the flash point. Ref. 64 lists the flash points of chemical compounds. The flash point differs from the fire point, i.e., the temperature at which the heated liquid will produce vapors sufficient to sustain continuous burning once

ignition has been started by an outside source. The term kindling temperature has the equivalent meaning for solids that the term fire point has for liquids. A few subliming solids, however, also have flash points.

The flash point is more significant than the fire point from the standpoint of safety since it indicates a lower limit of flammability. Both flash point and fire point are determined by laboratory procedures under stipulated conditions that might be different from actual field conditions. The difference between flash point and fire point might be considered a safety factor. The designer should keep in mind that materials kept at temperatures below the flash point, in normal operation, will present less of a fire hazard than if this temperature is exceeded. In Army systems it is next to impossible to keep fuels such as gasoline at temperatures below their flash points except in very cold climates and seasons.

The hazard ratings assigned by different agencies based on flash point tests vary. One of the most frequently used is the National Fire Protection Association's (NFPA) flash point scale (Ref. 64), which states that a liquid with a flash point of $-7°C$ (19°F) is very hazardous; $-7°$ to $21°C$ ($19°$ to $70°F$), moderately hazardous; $21°$ to $93°C$ ($70°$ to $199°F$), slightly hazardous; and above $93°C$ (above $199°F$), combustible. When the temperature of a liquid has exceeded the fire point, it is as dangerous as any flammable gas, and the flash point loses any significance regarding comparative hazards. Substances are classified based on flash points and hazard potential to establish tables of acceptable risk for storage. Table 10-36 is provided by the Industrial Indemnity Company (Ref. 41).

Coal is an example of a complex fuel. When heated, it gives off volatile gases that burn and, in so doing, furthers the oxidation of the carbon, which continues the process and feeds the fire. The carbon oxidizes to form carbon monoxide, which, in the presence of additional oxygen, burns to form carbon dioxide.

Other terms frequently encountered are autoignition temperature (AIT) or spontaneous ignition temperature (SIT). Both of these indicate the lowest temperature at which a flammable mixture or material will begin to self-heat at a high enough rate to result in combustion. Table 10-35 (Ref. 63) lists the AIT of flammable gaseous mixtures; additional data are contained in Ref. 65. A stochiometric mixture is one containing exactly complementary amounts of fuel and oxidizer, both of which will be totally consumed in the reaction and will leave no remnants when combustion ceases.

TABLE 10-35. LIMITS OF FLAMMABILITY OF INDIVIDUAL GASES AND VAPORS IN AIR AT ATMOSPHERIC PRESSURE (Ref. 63)

Combustible	Limits of flammability, volume-percent		T_L^b, °C	AIT^c, °C	Combustible	Limits of flammability, volume-percent		T_L^b, °C	AIT^c, °C
	LFL_{25}^a	UFL_{25}^a				LFL_{25}^a	UFL_{25}^a		
Acetal	1.6	10	37	230	n-Butyl formate	1.7	8.2	....	.....
Acetaldehyde	4.0	60	....	175	n-Butyl stearate	[4]0.3	....	....	355
Acetic acid	[1]5.4	....	40	465	Butyric acid	[4]2.1	....	....	450
Acetic anhydride	[2]2.7	[3]10	47	390	α-Butryolactone	[8]2.0	....	....	.....
Acetanilide	[4]1.0	....	....	545	Carbon disulfide	1.3	50	....	90
Acetone	2.6	13	....	465	Carbon monoxide	12.5	74	....	.....
Acetophenone	[4]1.1	....	....	570	Chlorobenzene	1.4	....	21	640
Acetylacetone	[4]1.7	....	....	340	m-Cresol	[8]1.1	....	....	.....
Acetyl chloride	[4]5.0	....	....	390	Crotonaldehyde	2.1	[11]16	....	.....
Acetylene	2.5	100	....	305	Cumene	[1]0.88	[1]6.5	....	425
Acrolein	2.8	31	....	235	Cyanogen	6.6	....	....	.....
Acrylonitrile	3.0	....	−6	.....	Cycloheptane	1.1	6.7	....	.....
Acetone cyanohydrin	2.2	12	....	.....	Cyclohexane	1.3	7.8	....	245
Adipic acid	[4]1.6	....	....	420	Cyclohexanol	[4]1.2	....	....	300
Aldol	[4]2.0	....	....	250	Cyclohexene	[1]1.2	....	....	.....
Allyl alcohol	2.5	18	22	.....	Cyclohexyl acetate	[4]1.0	....	....	335
Allyl amine	2.2	22	....	375	Cyclopropane	2.4	10.4	....	500
Allyl bromide	[4]2.7	....	....	295	Cymene	[1]0.85	[1]6.5	....	435
Allyl chloride	2.9	....	−32	485	Decaborane	0.2	....	....	.....
o-Aminodiphenyl	0.66	4.1	....	450	Decalin	[1]0.74	[1]4.9	57	250
Ammonia	15	28	....	.....	n-Decane	[12]0.75	[13]5.6	46	210
n-Amyl acetate	[1]1.0	[7]7.1	25	360	Deuterium	4.9	75	....	.....
n-Amyl alcohol	[1]1.4	[1]10	38	300	Diborane	0.8	88	....	.....
tert-Amyl alcohol	[4]1.4	....	....	435	Diesel fuel (60 cetane)	....	....	....	225
n-Amyl chloride	[5]1.6	[1]8.6	....	260	Diethyl amine	1.8	10	....	.....
tert-Amyl chloride	[6]1.5	....	−12	345	Diethyl analine	[4]0.8	....	80	630
n-Amyl ether	[4]0.7	....	....	170	1,4-Diethyl benzene	[1]0.8	....	....	430
Amyl nitrite	[4]1.0	....	....	210	Diethyl cyclohexane	0.75	....	....	240
n-Amyl propionate	[4]1.0	....	....	380	Diethyl ether	1.9	36	....	160
Amylene	1.4	8.7	....	275	3,3-Diethyl pentane	[1]0.7	....	....	290
Aniline	[7]1.2	[7]8.3	....	615	Diethyl ketone	1.6	....	....	450
Anthracene	[4]0.65	....	....	540	Diisobutyl carbinol	[1]0.82	[10]6.1	....	.....
n-Amyl nitrate	1.1	....	....	·195	Diisobutyl ketone	[1]0.79	[1]6.2	....	.....
Benzene	[1]1.3	[1]7.9	....	560	2-4, Diisocyanate	....	....	120	.....
Benzyl benzoate	[4]0.7	....	....	480	Diisopropyl ether	1.4	7.9	....	.....
Benzyl chloride	[4]1.2	....	....	585	Dimethyl amine	2.8	....	....	400
Bicyclohexyl	[1]0.65	[8]5.1	74	245	2,2-Dimethyl butane	1.2	7.0	....	.....
Biphenyl	[9]0.70	....	110	540	2,3-Dimethyl butane	1.2	7.0	....	.....
2-Biphenylamine	[4]0.8	....	....	450	Dimethyl decalin	[1]0.69	[9]5.3	....	235
Bromobenzene	[4]1.6	....	....	565	Dimethyl dichlorosilane	3.4	....	....	.....
Butadiene (1,3)	2.0	12	....	420	Dimethyl ether	3.4	27	....	350
n-Butane	1.8	8.4	−72	405	n,n-Dimethyl formamide	[1]1.8	[1]14	57	435
1,3-Butandiol	[4]1.9	....	....	395	2,3-Dimethyl pentane	1.1	6.8	....	335
Butene-1	1.6	10	....	385	2,2-Dimethyl propane	1.4	7.5	....	450
Butene-2	1.7	9.7	....	325	Dimethyl sulfide	2.2	20	....	205
n-Butyl acetate	[5]1.4	[1]8.0	....	425	Dimethyl sulfoxide	....	....	84	.....
n-Butyl alcohol	[1]1.7	[1]12	....	.....	Dioxane	2.0	22	....	265
sec-Butyl alcohol	1.7	[9]9.8	21	405	Dipentene	[8]0.75	[8]6.1	45	237
tert-Butyl alcohol	1.9	[9]9.0	11	480	Diphenylamine	[4]0.7	....	....	635
tert-Butyl amine	[1]1.7	[8]8.9	....	380	Diphenyl ether	[4]0.8	....	....	620
n-Butyl benzene	[1]0.82	[1]5.8	....	410	Diphenyl methane	[4]0.7	....	....	485
sec-Butyl benzene	[1]0.77	[1]5.8	....	420	Divinyl ether	1.7	27	....	.....
tert-Butyl benzene	[1]0.77	[1]5.8	....	450	n-Dodecane	[4]0.60	....	74	205
n-Butyl bromide	[1]2.5	....	....	265	Ethane	3.0	12.4	−130	515
Butyl cellosolve	[5]1.1	[10]11	....	245					
n-Butyl chloride	1.8	[1]10	....	.....					

See footnotes at end of table.

TABLE 10-35 (cont'd)

Combustible	Limits of flammability, volume-percent LFL25	Limits of flammability, volume-percent UFL25	T_L^b, °C	AIT^c, °C
Ethyl acetate	2.2	11	....	.....
Ethyl alcohol	3.3	[11]19	....	365
Ethyl amine	3.5	....	....	385
Ethyl benzene	[1]1.0	[1]6.7	....	430
Ethyl chloride	3.8	....	....	.....
Ethyl cyclobutane	1.2	7.7	....	210
Ethyl cyclohexane	[14]2.0	[14]6.6	....	260
Ethyl cyclopentane	1.1	6.7	....	260
Ethyl formate	2.8	16	....	455
Ethyl lactate	1.5	....	....	400
Ethyl mercaptan	2.8	18	....	300
Ethyl nitrate	4.0	....	....	.....
Ethyl nitrite	3.0	50	....	.....
Ethyl propionate	1.8	11	....	440
Ethyl propyl ether	1.7	9	....	.....
Ethylene	2.7	36	....	490
Ethyleneamine	3.6	46	....	320
Ethylene glycol	[4]3.5	....	....	400
Ethylene oxide	3.6	100	....	.....
Furfural alcohol	[15]1.8	[16]16	72	390
Gasoline:				
100/130	1.3	7.1	....	440
115/145	1.2	7.1	....	470
Glycerine	....	....	....	370
n-Heptane	1.05	6.7	−4	215
n-Hexadecane	[4]0.43	....	126	205
n-Hexane	1.2	7.4	−26	225
n-Hexyl alcohol	[1]1.2	....	....	.....
n-Hexyl ether	[4]0.6	....	....	185
Hydrazine	4.7	100	....	.....
Hydrogen	4.0	75	....	400
Hydrogen cyanide	5.6	40	....	.....
Hydrogen sulfide	4.0	44	....	.....
Isoamyl acetate	[1]1.1	[1]7.0	25	360
Isoamyl alcohol	[1]1.4	[1]9.0	....	350
Isobutane	1.8	8.4	−81	460
Isobutyl alcohol	[1]1.7	[1]11	....	.....
Isobutyl benzene	[10]0.82	[10]6.0	....	430
Isobutyl formate	2.0	8.9	....	.....
Isobutylene	1.8	9.6	....	465
Isopentane	1.4	....	....	.....
Isophorone	0.84	....	....	460
Isopropylacetate	[4]1.7	....	....	.....
Isopropyl alcohol	2.2	....	....	.....
Isopropyl biphenyl	[4]0.6	....	....	440
Jet fuel:				
JP-4	1.3	8	....	240
JP-6	....	....	....	230
Kerosene	....	....	....	210
Methane	5.0	15.0	−187	540
Methyl acetate	3.2	16	....	.....
Methyl acetylene	1.7	....	....	.....
Methyl alcohol	6.7	[11]36	....	385
Methyl amine	[4]4.2	....	....	430
Methyl bromide	10	15	....	.....
3-Methyl butene-1	1.5	9.1	....	.....

Combustible	Limits of flammability, volume-percent LFL25	Limits of flammability, volume-percent UFL25	T_L^b, °C	AIT^c, °C
Methyl butyl ketone	[5]1.2	[1]8.0	....	.....
Methyl cellosolve	[17]2.5	[7]20	....	380
Methyl cellosolve acetate	[8]1.7	....	46	.....
Methyl ethyl ether	[4]2.2	....	....	.....
Methyl chloride	[4]7	....	....	.....
Methyl cyclohexane	1.1	6.7	....	250
Methyl cyclopentadiene	[1]1.3	[1]7.6	49	445
Methyl ethyl ketone	1.9	10	....	.....
Methyl ethyl ketone peroxide	....	....	40	390
Methyl formate	5.0	23	....	465
Methyl cyclohexanol	[4]1.0	....	....	295
Methyl isobutyl carbinol	[4]1.2	....	40	.....
Methyl isopropenyl ketone	[5]1.8	[5]9.0	....	.....
Methyl lactate	[1]2.2	....	....	.....
α-Methyl naphthalene	[4]0.8	....	....	530
2, Methyl pentane	[4]1.2	....	....	.....
Methyl propionate	2.4	13	....	.....
Methyl propyl ketone	1.6	8.2	....	.....
Methyl styrene	[4]1.0	....	49	495
Methyl vinyl ether	2.6	39	....	.....
Methylene chloride	....	....	....	615
Monoisopropyl bicyclohexyl	0.52	[18]4.1	124	230
2-Monoisopropyl biphenyl	[10]0.53	[18]3.2	141	435
Monomethylhydrazine	4	....	....	.....
Naphthalene	[19]0.88	[20]5.9	....	526
Nicotine	[1]0.75	....	....	.....
Nitroethane	3.4	....	30	.....
Nitromethane	7.3	....	33	.....
1-Nitropropane	2.2	....	34	.....
2-Nitropropane	2.5	....	27	.....
n-Nonane	[21]0.85	....	31	205
n-Octane	0.95	....	13	220
Paraldehyde	1.3	....	....	.....
Pentaborane	0.42	....	....	.....
n-Pentane	1.4	7.8	−48	260
Pentamethylene glycol	....	....	....	335
Phthalic anhydride	[7]1.2	[22]9.2	140	570
3-Picoline	[4]1.4	....	....	500
Pinane	[23]0.74	[23]7.2	....	.....
Propadiene	2.16	....	....	.....
Propane	2.1	9.5	−102	450
1,2-Propandiol	[4]2.5	....	....	410
β-Propiolactone	[3]2.9	....	....	.....
Propionaldehyde	2.9	17	....	.....
n-Propyl acetate	1.8	8	....	.....
n-Propyl alcohol	[12]2.2	[1]14	....	440
Propyl amine	2.0	....	....	.....

See footnotes at end of table.

TABLE 10-35 (cont'd)

Combustible	Limits of flammability, volume-percent		T_L^b, °C	AIT^c, °C
	LFL$_{25}$ [a]	UFL$_{25}$ [a]		
Propyl chloride	[4]2.4	.....	.....	.....
n-Propyl nitrate	[17]1.8	[17]100	21	175
Propylene	2.4	11	.....	460
Propylene dichloride	[4]3.1	.....	.....	.....
Propylene glycol	[24]2.6	.....	.....	.....
Propylene oxide	2.8	37	.....	.....
Pyridine	[11]1.8	[25]12	.....	.....
Propargyl alcohol	[5]2.4	.....	.....	.....
Quinoline	[4]1.0	.....	.....	.....
Styrene	[26]1.1	.....	.....	....
Sulfur	[27]2.0	.....	247	....
p-Terphenyl	[4]0.96	.....	.....	535
n-Tetradecane	[4]0.5	.....	.....	200
Tetrahydrofurane	2.0	.....	.....	....
Tetralin	[1]0.84	[8]5.0	71	385
2,2,3,3-Tetramethyl pentane	0.8	.....	.....	430
Tetramethylene glycol	.....	.....	.....	390
Toluene	[1]1.2	[1]7.1	.....	480

Combustible	Limits of flammability, volume-percent		T_L^b, °C	AIT^c, °C
	LFL$_{25}$ [a]	UFL$_{25}$ [a]		
Trichloroethane	[28]12	[25].....	.....	500
Trichloroethylene	.....	[25]40	30	420
Triethyl amine	1.2	8.0	.....	.....
Triethylene glycol	[8]0.9	[28]9.2	.....	.....
2,2,3-Trimethyl butane	1.0	.....	.....	420
Trimethyl amine	2.0	12	.....	.....
2,2,4-Trimethyl pentane	0.95	.....	.....	415
Trimethylene glycol	[4]1.7	.....	.....	400
Trioxane	[4]3.2	.....	.....	.....
Turpentine	[1]0.7	.....	.....	.....
Unsymmetrical dimethylhydrazine	2.0	95	.....	.....
Vinyl acetate	2.6	.....	.....	.....
Vinyl chloride	3.6	33	.....	.....
m-Xylene	[1]1.1	[1]6.4	.....	530
o-Xylene	[1]1.1	[1]6.4	.....	465
p-Xylene	[1]1.1	[1]6.6	.....	530

[a] The sub "25" indicates a temperature of 25°C unless otherwise indicated by footnote.
[b] T_L = lower temperature limit
[c] AIT = autoignition temperature

[1] t = 100°C
[2] t = 47°C
[3] t = 75°C
[4] Calculated
[5] t = 50°C
[6] t = 85°C
[7] t = 140°C
[8] t = 150°C
[9] t = 110°C
[10] t = 175°C

[11] t = 60°C
[12] t = 53°C
[13] t = 86°C
[14] t = 130°C
[15] t = 72°C
[16] t = 117°C
[17] t = 125°C
[18] t = 200°C
[19] t = 78°C
[20] t = 122°C

[21] t = 43°C
[22] t = 195°C
[23] t = 160°C
[24] t = 96°C
[25] t = 70°C
[26] t = 29°C
[27] t = 247°C
[28] t = 30°C
[29] t = 203°C

TABLE 10-36. ACCEPTABLE FUEL STORAGE CONDITIONS (Ref. 41)

Container Type	Flammable Liquids			Combustible Liquids	
	Class 1A	Class 1B	Class 1C	Class II	Class III
Glass	1 pt	1 qt	1 gal	1 gal	5 gal
Metal (other than DOT Drums approved plastic)	1 gal	5 gal	5 gal	5 gal	5 gal
Safety Cans	2 gal	5 gal	5 gal	5 gal	5 gal

Class 1 Flammable Liquid means any liquid having a closed cup flash point below 37.8°C (100°F) and having a vapor pressure not exceeding 276 kPa (40 psi) (absolute) (2068.6 mm) at 37.8°C (100°F).

Class 1 Liquid can be subdivided as follows:

Class 1A—Flash points below 22.8°C (73°F), boiling point below 37.8°C (100°F)
Class 1B—Flash points below 22.8°C (73°F), boiling point above 37.8°C (100°F)
Class 1C—Flash points at or above 22.8°C (73°F) and below 37.8°C (100°F).

Combustible Liquid means a liquid having a flash point at or above 37.8°C (100°F). They are subdivided as follows:

Class II—Flash points at or above 37.8°C (100°F) and below 60°C (140°F)
Class IIIA—Flash points at or above 60°C (140°F) and below 93°C (200°F)
Class IIIB—Flash points at or above 93°C (200°F)

Reprinted with permission. Copyright © by Industrial Indemnity Company.

10-12.4 IGNITION SOURCES

When molecules of fuel and oxidizer in a mixture collide with sufficient velocity and force to initiate a reaction, ignition occurs. The activation energy sufficient to cause a reaction (ignition) is provided in the form of heat. Light or forms of mechanical energy transformed into heat can also cause initial dissociation of molecules and increase their velocities sufficiently to start a fire. Photons of light travel at extremely high velocities, and their impacts result in energy that may be sufficient to initiate reactions of such gas mixtures as hydrogen and chlorine. These gases will not react in darkness at room temperature but, if exposed to sunlight, will ignite violently.

Conversion of some types of mechanical energy will produce similar effects. Thus, the conversion of the mechanical energy in a physical impact may be sufficient to initiate reactions of such sensitive substances as hydrazine, acetylene, or initiators in weapons.

Common sources of ignition include open flames, electrical arcs or sparks, hot surfaces, mechanical or chemical sparks, spontaneous ignition, and adiabatic compression. The configuration of the energy source will have great influence upon the amount of energy required to initiate combustion. When a suitable gas mixture is present, the ignition source needs only to initiate a reaction in a very small volume. The heat emitted will then ignite surrounding gas. Less energy is needed to ignite a gas when a point source such as a flame or spark is introduced than is required with a diffuse source such as a hot surface.

Some examples of probable locations of the common sources of ignition are

1. *Open Flames.* The most common source of open flame—and a very frequent initiator of accidental fires—is matches used to light cigarettes. Other open flames are present as pilot lights for gas burners, in welding or cutting torches, and in open campfires.

2. *Electrical Arcs or Sparks.* A spark occurs when the potential between two conductors is great enough to overcome the resistance between the two so that electron flow is initiated. An electrical arc occurs when the potential remains high enough so that the electrons continue to flow through the intervening air or gas. Electrical arcs or sparks may arise from

a. The gaps between brushes and rotors of electric motors, generators, or other electrical rotating equipment

b. Between contacts of switches and relays that open to break the flow of current

c. Discharge of accumulated static electricity onto a nearby surface that is at a lower potential

d. Lightning strikes

e. Discharges of charged capacitors through a gaseous medium

f. Accidental contacts during a short circuit

g. Poor contacts between conductors, e.g., light bulbs poorly fitted into sockets or loose connectors (plugs and socket combinations)

h. Breaking or cutting of conductors carrying electrical currents

i. Electric welding.

3. *Hot Surfaces.* Hot surfaces that might serve as ignition sources are numerous and common. Some will cause ignition only after prolonged exposure, either because the heat buildup must reach a certain temperature to induce combustion or because the heat will cause eventual decomposition of the flammable material into more reactive substances. Decomposition might break down heavy oils into less complex, more reactive molecules that are easier to ignite at lower temperatures than the original product. Probably the most common cause of accidental fires by a hot surface is ignition of a combustible substance by a lighted cigarette carelessly discarded. The lighted cigarette can also be considered a tiny, open flame. Other igniting hot surfaces include

a. Electric heaters and hot plates

b. Components of operating engines or compressors, especially the exhaust manifolds and catalytic converters

c. Overheated electrical wiring, motors, heaters (especially when thermostats fail and heaters remain on), or other equipment

d. Boiler and furnace surfaces, stacks, chimneys

e. Friction-heated surfaces, including brake drums (they can become red hot and visibly so in bright sunlight), and bearings

f. Surfaces heated by intense light from lasers or fires

g. Surfaces being welded or being cut by welding torches

h. Hot process equipment.

4. *Mechanical and Chemical Sparks.* Mechanical sparks are produced by friction between hard materials or substances, such as steel tools being sharpened on a grinding wheel, aircraft making wheels-up landings on runways, or ground vehicles negotiating rocky surfaces in rough terrain. Soft metals will not spark. To spark, a metal must have three basic properties:

a. The metal must be of such composition that the energy required to create particles through friction will be great enough to heat those particles to high temperatures.

b. The metal must oxidize and burn easily. (Metals with this property are highly electropositive.)

c. The metal must have a low specific heat.

Examining the tables of properties of materials for sparking characteristics will enable the design engineer to specify nonsparking tools or to determine when the choice of a metal will minimize sparking hazards. Bronze tools, for example, are commonly used in areas containing explosives. Generally, materials that clog grinding wheels are nonsparking—e.g., aluminum, copper, bronze, brass, zinc and tin alloys (pot metal), and pewter (tin and lead). A chemical spark is a very hot—usually incandescent—solid particle. The most common example is glowing carbon emitted from an internal combustion engine because of incomplete combustion. These hot particles constitute a fire hazard and require the use of spark arresters on some Army equipment.

5. *Spontaneous Ignition.* Under certain conditions some substances (fuel) will react with oxygen from the air (or other substances). The heat from this reaction will raise the temperature of the substance to the fire point, and the fuel will ignite "spontaneously". There are a number of means by which this "spontaneity", or self-ignition, can occur, namely,

a. Easily oxidizable substances such as petroleum products will react slowly with the oxygen in air and generate heat that accumulates until the temperature finally reaches the autoignition point. In Army systems the commonest occurrence of such spontaneous ignition is with oily rags. These can be found in tanks and other vehicles when maintenance is performed; when these rags are not properly stored in closed containers to isolate them from the air, fires occur.

b. For special purposes such as in liquid-fueled rockets, the fuels selected will react so violently with their oxidizers and will produce so much heat that no other ignition source is needed. A fuel and oxidizer that react in this fashion are said to be hypergolic. Hydrazine and unsymmetrical dimethyl hydrazine (UDMH), used as propellants in an Army missile, are hypergolic. The principal advantage is that no ignition source is needed. Red fuming nitric acid (RFNA) is an example of an oxidizer used to provide the hypergolic combination for rocket propulsion. These substances are extremely hazardous to personnel and equipment when spilled or otherwise leaked to the uncontrolled state.

c. When a fuel is hypergolic with the oxygen in air, the fuel is said to be pyrophoric. The element phosphorus is an example.

d. Adiabatic compression occurs when a gas is compressed and the energy of compression is retained in the gas. This process causes the temperature of the gas to rise. If the compression occurs in a manner which also provides an oxygen source, the vapor will ignite when the autoignition temperature is reached. With a slight variation, this is the process that causes the diesel engine to operate. The difference is that in a diesel engine the fuel is not present during the compression of the air but is later injected into the compressed, heated air, where the mist of fuel is rapidly turned to vapor at its autoignition temperature.

6. *Radiation.* Radiation of heat energy is another source of ignition of flammable materials. For most solids it is necessary that the surface be heated to provide the flammable vapor for combustion. With solid propellants the radiation from the flames to the surface of the solid propellant provides the heat that causes the propellant to melt and vaporize. Laser beams are another source of radiant energy adequate to initiate fires if combustible materials are present.

10-12.5 HAZARD CONTROL TECHNIQUES

Designers can minimize the occurrence of accidental fires by using the least flammable substance that will accomplish the required mission and keep fuels away from oxidizers and ignition sources away from flammable mixtures. The design engineer should adopt design goals of

1. Keeping operating temperatures as low as possible to avoid igniting easily combustible materials or creating environments in which less combustible materials can be easily ignited

2. Increasing the distances between ignition sources and combustibles

3. Eliminating the use of substances capable of hypergolic or pyrophoric reactions or self-igniting oxidation (spontaneous combustion)

4. Keeping thermal energy levels at the lowest effective level

5. Avoiding unknown combinations of reactive chemicals without performing theoretical analyses of possible adverse effects

6. Using the least reactive substances possible.

10-12.6 FIRE SUPPRESSION

The designer's role in fire suppression is to consider the potential hazards to personnel and equipment of the system under development and of the environment in which this equipment is to be used. Fire-suppressant features can then be designed into the equipment. Alternatively, mobile extinguishers of the correct type must be incorporated into the design specification, and provision for their placement and use must be provided for in the design. Without designer consideration and recommendations, logistic action to provide the correct extinguishant cannot be taken.

Fires are not uncommon because materials that are also fuels must necessarily be used in the fabrication of Army systems, because of the almost certain presence of air containing oxygen, and because of the frequent presence of an ignition source. It is advisable, therefore, that provisions be made to combat the accidental fires that may occur. If one of the four elements necessary for fires can be eliminated or changed in some manner, the risk of fire can be greatly reduced. Some of the ways to achieve this objective are

1. *Fuel.* Sometimes provisions can be designed into systems to stop the flow of fuel into an unwanted fire by means of an automatic or manually operated valve in the feed line. When the valve is shut, the fire exhausts itself for lack of fuel.

2. *Oxidizer.* Blanketing a fire to deny it the oxygen present in air is the commonest method. The principal means is by use of a foam, which covers, or smothers, the fire.

3. *Flammable Mixture.* Eliminating the fuel or oxidizer is the most common example of this method; however, there are other means. One is to dilute the mixture with an inert gas such as nitrogen so that the reactive particles cannot strike each other often enough to sustain the reaction. Another method is to cool the fire. That has two effects: The first is to reduce the temperature of the fuel so that vapors adequate to maintain a flammable mixture are not generated, and the second effect of cooling is discussed in Item 4, "Ignition", which follows. Another means, developed since the initial studies of chain reactions, is to provide a material that interferes with the chain. Carbon dioxide is one such material, but even more effective are the halogenated hydrocarbons, some of which are a proprietary group of substances with the trade name "Halons". With halogenated hydrocarbons, the reaction is diverted from the usual chain into a self-defeating direction. Very small amounts of such halogenated hydrocarbons are highly effective. Table 10-37 (Ref. 66) compares the required peak percentage by volume of three extinguishing agents necessary to extinguish the burning of some combustibles in air. The extinguishing agents are a halogenated hydrocarbon, methyl bromide; nitrogen; and carbon dioxide. Table 10-37 shows the superiority of the halogenated hydrocarbon followed by carbon dioxide. The newer combinations of Halons (1211) are less hazardous from a toxic vapor standpoint than methyl bromide.

TABLE 10-37. COMPARISON OF EXTINGUISHING POWER OF METHYL BROMIDE, NITROGEN, AND CARBON DIOXIDE (Ref. 66)

Combustible (In Air)	Methyl Bromide	Nitrogen	Carbon Dioxide
	Peak Percentage by Volume		
Hydrogen	13.7	75	61
Carbon Monoxide	6.2	68	52
Ethylene	11.65	50	41
Methane	4.7	38	25
n-Hexane	7.05	42	29
Benzene	7.75	44	31

4. *Ignition.* Cooling will lower the temperatures of flames and other sources of heat from which flammable mixtures can be ignited. Cooling can stop the ignition or prevent its occurrence. The use of water on a fire is the most common example.

10-12.7 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

DoD specifications and standards that contain design requirements for prevention of fires are listed in Table

10-38. Many of these design requirements relate indirectly to the prevention of fires, but the specific fire prevention design requirements include

1. Exhausts from engines will be reduced in temperature so as not to cause ignition of a flammable atmosphere.

2. Spark arresters will be used on exhausts of engines operated in flammable environments.

3. Equipment or materials will not emit gases that could create a flammable atmosphere.

TABLE 10-38. GOVERNMENT DOCUMENTS CONTAINING DESIGN REQUIREMENTS THAT ASSIST IN FIRE PREVENTION

MIL-E-4158	Electronic Equipment, Ground, General Requirements for
B-5087	Bonding, Electrical and Lightning Protection for Aerospace Systems
W-5088	Wiring, Aerospace Vehicle
E-5400	Electronic Equipment, Aerospace, General Specification for
H-5440	Hydraulic Systems, Aircraft, Types I and II, Design and Installation Requirements
P-5518	Pneumatic Systems, Aircraft, Design, Installation, and Data Requirements for
E-6051	Electromagnetic Compatibility Requirements, System
E-7080	Electrical Equipment, Aircraft, Selection and Installation of
W-8160	Wiring, Guided Missile
E-8189	Electronic Equipment, Missiles, General Specification for
S-8512	Support Equipment, Aeronautical, Special
P-8564	Pneumatic System Components, Aeronautical
I-8700	Installation and Test of Electronic Equipment in Aircraft
H-8775	Hydraulic System Components, Aircraft and Missiles
E-11991	Electronic, Electrical and Electromechanical Equipment Missile
S-23069	Safety Requirements, Minimum, for Air Launched Guided Missiles
E-25366	Electrical and Electronic Equipment Guided Missile
T-28800	Test Equipment for Use With Electrical and Electronic Equipment
L-11992	Launchers for Guided Missiles, Ground and Airborne, General Specifications for
I-23659	Initiators, Electric, General Design Specification
R-23139	Rocket Motors, Surface Launched, Development and Qualifications for
MIL-STD-415	Test Provisions for Electronic Systems and Associated Equipment, Design Criteria for
454	Standard General Requirements for Electronic Equipment
648	Design Criteria for Specialized Shipping Containers
810	Environmental Test Methods & Engineering Guidelines
882	System Safety Program Requirements
1365	General Design Criteria for Handling Equipment Associated With Weapons and Related Items
1385	Preclusion of Ordnance Hazards in Electromagnetic Fields, General Requirements for
1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
1512	Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
1316	Fuzes, Navy, Design Safety, Criteria for
AFSC DH 1-6	System Safety
AFSC DH 2-5	Ordnance Systems
OSHA STDS	Occupational Safety and Health Standards
TITLE 21 CFR	Part 1040 Performance Standards for Light-Emitting Products
DOD Manual	
4145.26	DOD Contractors' Safety Manual for Ammunition, Explosives, and Related Dangerous Material

4. If substances constituting a fire and/or explosion hazard are present, they will be kept separated from heat sources, spark arresters will be incorporated, suitable vents and drains will be provided, and other fire prevention measures will be taken as necessary for the circumstances.

5. Equipment will not be capable of causing ignition of an ambient explosive gaseous mixture with air when operating in such an atmosphere.

6. Wiring will be protected from overheating by fuses or circuit breakers.

7. Bonding and grounding will be designed into the equipment in accordance with the environment in which it will operate.

8. Materials used in equipment will be fire resistant to the maximum extent possible that is consistent with military performance requirements.

9. Unless specifically exempted by the Army command responsible for development of the equipment, the system will be designed to meet the provisions of the National Electrical Code (NEC).

Fig. 10-38 (Ref. 41) provides information regarding the types of fires, i.e., types of combustible materials, and the type of fire extinguisher to use for each material. Installed or portable Halon extinguishers have the advantage of not damaging equipment or materials and of allowing operators more time to exit after use than do the carbon dioxide or other asphyxiant gas types.
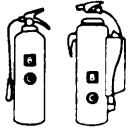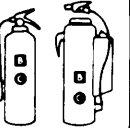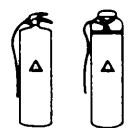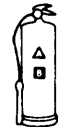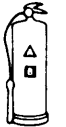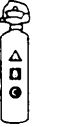
10-13 EXPLOSION

10-13.1 GENERAL

An explosion is a chemical reaction or change of state that occurs in an exceedingly short space of time with the generation of high temperature and, generally, a large volume of gas accompanied by a shock wave in the surrounding media. Materials developed intentionally to produce these effects are called "explosives". Other substances, however, such as finely divided coal or flour dust can accidentally become explosive because of the state of the environment in which they momentarily exist, although the individual constituents are usually nonexplosive. Characteristics of explosions vary according to the reacting substance, the confinement, and environmental conditions.

The substances specifically created for use as Army explosives fall into two categories, i.e., low and high explosives. Although all explosives have certain similar characteristics, other characteristics are peculiar to either low or high explosives. One common characteristic has been pointed out, i.e., that all explosives produce large amounts of gas in a short time. Another characteristic of an Army explosive—whether a mixture or a compound— is that it does not depend on the oxygen in air for a reaction.

Black powder is an example of a low explosive. Low explosives deflagrate, i.e., they burn rapidly, but the

Reprinted with permission. Copyright © by Industrial Indemnity Company.

Figure 10-38. Fires and Fire Extinguishers (Ref. 41)

reaction progresses through the material at a speed less than that of sound. If the explosive is not burned in a container and the resulting gas is unconfined, the deflagration will merely produce a fireball and a very minor overpressure or mild shock wave may occur as the gases expand rapidly. If the gases are confined, however, they may generate pressures great enough to rupture the container and generate a shock wave. The deflagration phenomenon is not limited exclusively to low explosives; trinitrotoluene (TNT) will deflagrate when loosely confined. Burning is a method of disposing of waste, unconfined explosives. Extreme precautions must be

taken, however, because of the possibility that the high explosive may explode. Certain high initiating explosives— lead azide, mercury fulminate, lead stryphnate, and tetracene—will not deflagrate; when exposed to sufficient activating energy, they will detonate. Detonation is the generation of an explosion or a shock wave that travels through the explosive itself at an extremely high speed— 6700 to 8380 m/s (22,000 to 27,500 ft/s). The front of the shock wave causes the adiabatic compression and initiation of the explosive material that it reaches. Thus the detonation of a high explosive occurs so rapidly that the unreacted material has no opportunity to break away from the unreacted mass.

Detonation will fail to occur in an unconfined explosive if its dimensions are below a specific (critical) lower limit. This is normally referred to as a critical diameter—on the order of a few centimeters or less for most explosives and for propellants that have shown to be detonatable. Some

substances, ammonium nitrate being noteworthy, require a very large mass to propagate a detonation (Ref. 67). The detonation of bulk quantities of ammonium nitrate with catastrophic results has been reported.

The sensitivity of crushed or shattered material is usually much higher than that of the highly consolidated material. Propellants that cannot be detonated under violent initiation conditions may be expected to become comparable to ordinary explosives in sensitivity when in a finely divided form (Ref. 67).

The physical, chemical, thermal, detonating, and electrical properties; sensitivity; and toxicity of low and high explosives may be found in Ref. 68.

Information on pure explosive compounds, cast explosives, plastic-bonded explosives, miscellaneous explosives, and additives and binders is contained in Tables 10-39 through 10-43 (Ref. 68), respectively.

TABLE 10-39. PURE EXPLOSIVE COMPOUNDS (Ref. 68)

Material	Chemical Name	Other Designations	Color
AN	Ammonium nitrate		Clear
AP	Ammonium perchlorate		White
BTF	Benzotris [1, 2, 5] oxadiazole, 1, 4, 7-trioxide	Benzotrifuroxan; Hexanitrosobenzene; Benzotrifurazan-N-oxide	Buff
DATB	2, 4, 6-Trinitro-1, 3-benzenediamine	1, 3-Diamino-2, 4, 6-trinitrobenzene	Yellow
DEGN	2, 2'-Oxybisethanol, dinitrate	Diethylene glycol dinitrate; Dinitrodigylcol	Clear
DIPAM	2, 2', 4, 4', 6, 6'-Hexanitro-[1, 1-biphenyl]-3, 3'-diamine	3, 3'-Diamino-2, 2', 4, 4', 6, 6'-Hexanitrobiphenyl; Hexanitrodiphenyl amine hexite; Dipicramide	—
DNPA	2, 2-Dinitropropyl acrylate		Off-white
EDNP	Ethyl 4, 4-dinitropentanoate	Ethyl 4, 4-dinitrovalerate	Yellow
Explosive D	Ammonium picrate	Dunnite	Yellow/red
FEFO	1, 1'-[Methylenebis(oxy)] bis[2-fluoro-2, 2-dinitroethane]	Bis(2-fluoro-2, 2-dinitroethyl) formal	Straw
HMX	Octahydro-1, 3, 5, 7-tetranitro-1, 3, 5, 7-tetrazocine	1, 3, 5, 7-Tetranitro-1, 3, 5, 7-tetrazacyclooctane; Cyclotetramethylene tetranitramine; Octogen	White
HNAB	Bis(2, 4, 6-trinitrophenyl)-diazene	2, 2', 4, 4', 6, 6'-Hexanitroazo-benzene	Reddish-orange
HNS	1, 1'-(1, 2-Ethenediyl)bis[2, 4, 6-trinitrobenzene]	2, 2', 4, 4', 6, 6'-Hexanitrostilbene	Yellow

TABLE 10-39. (cont'd)

Material	Chemical Name	Other Designations	Color
Lead azide			White
Lead styphnate	2, 4, 6-Trinitro-1, 3-benzenediol, lead salt	Lead trinitroresorcinate	Orange-yellow/brown
NC (12% N)	Partially nitrated cellulose	Nitrocellulose (lacquer grade); Cellulose trinitrate; Piroksilin; Pyroxylin	White
NC (13.35% N, min)	Partially nitrated cellulose	Nitrocellulose; Guncotton	White
NC (14.14% N)	Partially nitrated cellulose		White
NG	1, 2, 3-Propanetriol, trinitrate	Nitroglycerin; Glycerolnitrate	Clear
NM	Nitromethane		Clear
NQ	Nitroguanidine	Picrite	White
PETN	2, 2-Bis[(nitrooxy)methyl]-1, 3-propanediol, dinitrate	Pentaerythritol tetranitrate; Penthrite; TEN; Nitropenta	White
Picric acid	2, 4, 6-Trinitrophenol	Melinite; Perlit; Lyddit; 1-Hydroxy-2, 4, 6-trinitrobenzene	Yellow
RDX	Hexahydro-1, 3, 5-trinitro-1, 3, 5-triazine	1, 3, 5-Trinitro-1, 3, 5-triaza-cyclohexane; Cyclotrimethylene trinitramine; Hexogen; Cyclonite; Gh; T4; 1, 3, 5-Trinitro-trimethylenetriamine	White
TACOT	2, 4, 8, 10-Tetranitro-5H-benzo-triazolo-[2, 1-a]-benzotriazol-6-ium, hydroxide, inner salt	Tetranitrodibenzo-1, 3a, 4, 6a-tetrazapentalene	Red-orange
TATB	2, 4, 6-Trinitro-1, 3, 5-benzenetriamine	1, 3, 5-Triamino-2, 4, 6-trinitrobenzene	Bright yellow
Tetryl	N-Methyl-N, 2, 4, 6-tetranitro-benzenamine	2, 4, 6-Trinitrophenyl-methylnitramine; N-methyl-N, 2, 4, 6-tetranitroaniline; Tetranitro-methylaniline; Pyronite; CE	Yellow/buff
TNM	Tetranitromethane		Clear
TNT	2-Methyl-1, 3, 5-trinitrobenzene	2, 4, 6-Trinitrotoluene; Trotyl; T; Tolit	Buff/brown

TABLE 10-40. CAST EXPLOSIVES (Ref. 68)

	Formation, wt%			
			Other Ingredients	
Explosive	TNT	RDX	material	%
Amatol 80/20	20	—	AN	80
Baratol	24	—	Ba(NO₃)₂	76
Boracitol	40	—	Boric acid	60
Comp A-3	—	91	Wax	9
Comp A-5	—	98.5-99	Stearic acid	1.5-1
Comp B, Grade A	36	63	Wax	1
Comp B-3	40	60		
Cyclotol 75/25	25	75		
Cyclotol 60/40	40	60		
H-6	30	45	Al	20
			Wax	5
			(CaCl₂	0.5)
HBX-1	38	40	Al	17
			Wax	5
			(CaCl₂	0.5)
HBX-3	29	31	Al	35
			Wax	5
			(CaCl₂	0.5)
Minol-2	40	—	Al	20
			AN	40
Octol	25	—	HMX	75
Pentolite	50	—	PETN	50
Tritonal	80	—	Al	20

TABLE 10-41. PLASTIC-BONDED EXPLOSIVES (Ref. 68)

		Formation		
Explosive	Other Designations	Ingredient	wt%	Color
LX-04-1	PBHV-85/15	HMX	85	Yellow
		Viton A	15	
LX-07-2	RX-04-BA	HMX	90	Orange
		Viton A	10	
LX-09-0	RX-09-CB	HMX	93	Purple
		pDNPA	4.6	
		FEFO	2.4	
LX-09-1		HMX	93.3	Purple
		pDNPA	4.4	
		FEFO	2.3	

TABLE 10-41. (cont'd)

Explosive	Other Designations	Formation Ingredient	wt%	Color
LX-10-0	RX-04-DE	HMX Viton A	95 5	Blue-green spots on white
LX-10-1	RX-04-EA	HMX Viton A	94.5 5.5	Blue-green spots on white
LX-11-0	RX-04-PI	HMX Viton A	80 20	White
LX-14-0	RX-04-EQ	HMX Estane 5702-Fl	95.5 4.5	Violet spots on white
LX-15	RX-28-AS	HNS-I Kel-F 800	95 5	Beige
LX-16	RX-15-AD	PETN FPC 461	96 4	White
LX-17-0	RX-03-BB	TATB Kel-F 800	92.5 7.5	Yellow
PBX-9007	PBX-9007 Type B	RDX Polystyrene DOP Rosin	90 9.1 0.5 0.4	White or mottled gray
PBX-9010		RDX Kel-F 3700	90 10	White
PBX-9011	X-0008	HMX Estane 5703-Fl	90 10	Off-white
PBX-9205		RDX Polystyrene DOP	92 6 2	White
PBX-9404	PBX-9404-03	HMX NC (12.0% N) CEF	94 3 3	White or blue
PBX-9407		RDX FPC 461	94 6	White or black
PBX-9501	X-0242	HMX Estane BDNPA-F	95 2.5 2.5	White
PBX-9502	X-0290	TATB Kel-F 800	95 5	Yellow
PBX-9503	X-0351	HMX TATB Kel-F 800	15 80 5	Purple
PBX-9604	RX-10-AB	RDX Kel-F 800	96 4	—

TABLE 10-42. MISCELLANEOUS EXPLOSIVES (Ref. 68)

Explosive	Other Designations	Formation		Color
		Ingredient	wt%	
Black powder	Black gunpowder	KNO_3	75	Gray to black
		Charcoal	15	
		Sulfur	10	
Comp C-3		RDX	77	Yellow
		TNT	4	
		DNT	10	
		MNT	5	
		Tetryl	3	
		NC	1	
Comp C-4	Harrisite	RDX	91	Light brown
		Di-(2-ethylhexyl) sebacate	5.3	
		Polyisobutylene	2.1	
		Motor oil	1.6	
EL-506A	Detasheet	PETN	85	Red
		Binder	15	
EL-506C	Detasheet	PETN	63	Olive
		NC (12.3% N)	8	
		ATBC	29	
LX-01	NTN, RX-01-AA	NM	51.7	Clear
		TNM	33.2	
		1-Nitropropane	15.1	
LX-02-1	EL-506 L-3	PETN	73.5	Buff
	RX-02-AC	Butyl rubber	17.6	
		ATBC	6.9	
		Cab-O-Sil	2.0	
LX-08	RX-02-AM	PETN	63.7	Blue
		Sylgard 182	34.3	
		Cab-O-Sil	2.0	
LX-13		PETN	80	Green
		Sylgard 182	20	
MEN-11	RX-01-AC	NM	72.2	Clear
		Methanol	23.4	
		Ethylenediamine	4.4	
XTX-8003	Extex	PETN	80	White
		Sylgard 182	20	
XTX-8004	X-0208	RDX	80	White
		Sylgard 182	20	

TABLE 10-43. ADDITIVES AND BINDERS (Ref. 68)

Material	Chemical Name	Other Designations	Color
BDNPA-F	Bis(2, 2-dinitropropyl) acetal/bis(2, 2-dinitropropyl) formal, 50/50 wt%		Straw
Cab-O-Sil M-5		Amorphous silicon oxide	White
CEF	Tris-β-chloroethylphosphate		Clear
DOP	Di(2-ethylhexyl) phthalate	Dioctylphthalate	Clear
Estane 5702-F1		Polyurethane solution system	Light amber
FPC 461	Vinyl chloride/chlorotri-fluoroethylene copolymer, 1.5:1		White
Kel-F 800	Chlorotrifluoroethylene/vinyli-dine fluoride copolymer, 3:1		Off-white
Polystyrene			Clear
Sylgard 182	Poly(dimethylsiloxane)	Silicone resin	Light straw
Viton A	Vinylidine fluoride/hexa-fluoropropylene copolymer, 60/40 wt%		White

10-13.2 TOLERANCE AND SAFE EXPOSURE LIMITS

DARCOM-R 385-100 (Ref. 67) provides detailed information on

1. Explosive classes, divisions, and groups
2. Properties, use, and safety precautions relative to incorporating various explosives into ordnance designs
3. Storage of explosives
4. Quantity-distance requirements for explosives
5. Compatibility of types of explosives for storage
6. Restrictions and requirements for transporting explosives by rail, truck, air, and water.

The detailed information is not repeated here since it is so completely and conveniently presented in Ref. 67.

10-13.3 POTENTIAL HAZARD SOURCES

Army weapon systems contain explosive materials; consequently, they are potential sources of accidents. In addition, Army equipment frequently must be designed to withstand the effects of explosions intentionally generated by enemy actions. Injuries can result from use of explosives even when there are no accidents and equipment is functioning properly. For example, early in World War II, personnel firing large naval guns and artillery pieces were being burned because they had removed clothing or were not otherwise protected from the flames and heat generated during firing. Protective clothing and shields had to be provided. Ear protection had to be used to protect gunners' ears against injury.

Explosions involving Army systems do occur inadvertently. For example, blocked gun tubes, double charges of projectile propellants, or other factors (See Chapter 8.) may cause violent ruptures of artillery pieces. The high explosives (bursting charges) in Army use are relatively stable; the principal problem of accidental initiation of such explosives occurs with the less stable explosives in initiators. Similarly, problems with low explosives used as propellants are due principally to failures of initiating devices.

Explosions of materials that are not classed as explosives may occur with certain gases, which will detonate under highly adverse conditions or concentrations. There are few of these in Army systems. Hydrogen gas can accumulate in closed compartments and may reach explosive concentrations in battery shops or when trapped under vehicle engine hoods or battery compartment enclosures. Gasoline vapor is heavier than air, and leaking fuel in any vehicle can cause a buildup of explosive vapor as the gasoline vapor "flows" to lower, possibly confined, volumes of space. Liquid oxygen spilled onto asphalt or a similar organic substance results in the creation of an extremely sensitive explosive material. It is reported (Ref. 69) that a wrench dropped on such a spill resulted in a violent explosion with fatalities.

10-13.4 HAZARD CONTROL TECHNIQUES

Accidental initiations of explosives are minimized by engineering designs that satisfy military standards relating to the design of initiating control devices such as fuzes and safing and arming devices. The control techniques required for Army missiles provide good ordnance design guidance. The information, excerpted from MICOMP 385-4, *Safety, Ignition Systems for Army Rockets and Missiles* (Ref. 70), follows:

"5. *Safety Design Principles.* Some of the safety design principles that must be considered in the design of an ignition system for a missile system are:

"a. Isolate the igniter from the power source until such time that it must be intentionally actuated.

"b. Use the least sensitive igniters that will meet system requirements. As a minimum the National Ranges requirement that all Category 'A' electrical initiators have a no-fire level of at least one ampere and the capability to dissipate one watt for five minutes without degradation should be met. Category 'A' initiators are those which by the expenditure of their own energy or because they initiate a chain of events may cause injury or death to people or damage to property.

"c. Protect the system against accidental switch activation.

"d. Protect the system against RF energy, static electricity and other spurious electrical signals. MIL-STD-1316, *Fuze Design, Safety Criteria for* [Ref. 71], contains general safety objectives for Army ordnance as well as detailed design requirements for safety. The fuze techniques for control of explosive hazards are best defined by quoting the 'objectives' paragraph of this standard as follows:

"5.1 *General.* The features, procedures, or controls listed as objectives in this section are to be accepted as requirements in the design of fuzes covered by the scope of this document when achievement is within the state-of-the-art of fuze development and is feasible within the scope of development. Necessity for deviations from these objectives shall be documented, showing that compliance is not feasible.

"5.2 *Design features*

"5.2.1 *Stored energy.* The fuze safety system should not incorporate a stored energy mechanism which is used to remove an interrupter of the fuze explosive train unless no adequate environmental force is available to remove the interruption.

"5.2.2 *Fail-safe features.* Fuze systems should incorporate fail-safe features based on their applicability to system requirements.

"5.2.3 *Explosive ordnance disposal.* Fuzes should incorporate Explosive Ordnance Disposal (EOD) features based on the applicability of EOD to operational system requirements. (See AFR 136-8.)

"5.2.4 *Inspection and test.* The design of the fuze should facilitate the use of inspection and test equipment for visual, physical, or electronic monitoring of all characteristics which assure the safety and intended functioning of the fuze at all appropriate stages. The fuze design should facilitate the use of automatic inspection equipment. Design considerations should include possible connections with the weapon in-flight telemetry test devices.".

Refs. 72 and 73 also provide guidance for the design of timing mechanisms and fuzes, respectively.

In addition, the various items of Army ordnance are classified according to the degree of hazard presented by inadvertent initiation of the ordnance. TB 700-2 (Ref. 74) contains administrative and test procedures and the detailed test criteria to classify explosives. DARCOM-R 385-100 (Ref. 67) contains detailed technical information on many background subjects involved in insuring the safety of Army explosives. This manual should be reviewed by any engineer engaged in the design of explosive ordnance items.

In addition to a system of classifying Army explosives, it is necessary to consider the compatibility of different explosives in storage. Designers should be familiar with the compatibility requirement and the factors that determine compatibility. In other words, items that are stored together must get along well together. Previous experience with fires and explosions has revealed that certain types of explosives should be separated in storage. To be stored together in one place, two items must have comparable hazard potentials. For example, both a fragmentation bomb and a demolition charge are filled with high explosives; yet they are not considered compatible. This is because each has a different hazard potential. Although both items contain blast-producing explosives, the fragmentation bomb presents the additional hazard of high-velocity fragments upon detonation. Therefore, these two items are not normally stored together. Explosives are grouped for compatibility upon the basis of the following eight factors (Ref. 67):

1. Chemical and physical properties
2. Inner and outer packaging configuration
3. Design characteristics
4. Hazard classification
5. Rate of deterioration
6. Net explosive weight
7. Sensitivity to initiation
8. Effects of deflagration, explosion, or detonation.

For more detailed information refer to Ref. 67.

10-13.5 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

Since Army weapon systems all contain some form or type of explosive—propellant, bursting charge, fuze, pyrotechnic—the potential for a devastating accident is

always present. To reduce the accident potential, the design should be as safe as possible consistent with the mission. Weapons introduced into the stockpile—having been subjected to explosive testing—are extremely safe if handled under prescribed conditions. Accordingly, the designed-in safety can be preserved and enhanced by applying proper procedure—i.e., field and technical manuals and standard operating procedures. Good, documented procedures are the cornerstone of safe operations with propellants and explosives. Proper instruction and education in the application of the instructions will result in well indoctrinated and trained users.

Assume that the weapon has been type classified and handled in accordance with documented procedures; then the most likely source of a catastrophic accident is a malfunctioning safing and arming mechanism and/or fuze—even though extremely remote—over which the user has no control. To insure maximum safety in fuzes, the design principles of MIL-STD-1316, *Fuze Design, Safety Criteria for* (Ref. 71), must be adhered to. Refs. 71 and 72, design handbooks for timing mechanisms and fuzes, respectively, implement the provisions of Ref. 71. Before engaging in fuze and/or safing and arming design, the engineer should consult these references.

Finally, to make the safety procedure complete, every accident involving explosives should be reported and investigated, regardless of how trivial or minor.

10-14 ELECTRICAL HAZARDS

Electrical hazards may be categorized in numerous ways. Here, electrical hazards have been divided into seven principal categories, and each is discussed at length:
1. Electrical shock
2. Ignition of combustible material
3. Heating and overheating
4. Inadvertent activation
5. Failure to operate as required
6. Electrical explosions
7. Static electricity.

These seven categories may overlap; for example, static electricity can cause inadvertent activation of electro-explosive devices or ignition of combustible materials. Electrical hazards are almost all man-made since the only electricity available naturally is from static electric sources, including—on a large scale—lightning.

Electricity usually originates at commercial sources, but in most Army systems it is provided by engine-driven-generator sets or batteries. Electricity from these sources is of two types, i.e., alternating current (ac) and direct current (dc). Alternating current is generated at various voltages and at frequencies of 50, 60, and 400 Hz—and in special cases at higher frequencies.

The hazards and safeguards of electricity depend on the frequency, voltage, current, and other factors, all of which are described in the paragraphs that follow.

10-14.1 ELECTRICAL SHOCK

Electrical shock is the sudden and accidental stimulation of the body's nervous system by an electric current. Whenever the human body becomes part of an electrical circuit, current will flow through the body. The amount of current will depend on the potential difference and the body's resistance to current flow. There are three variables in an electrical circuit: current, voltage, and resistance, which are interrelated by Ohm's law

$$V = RI, \text{ V} \qquad (10\text{-}5)$$

where
V = voltage, V
R = resistance, Ω
I = current, A.

Therefore, when a body becomes part of a circuit, the amount of current that flows through the body will depend upon the resistance of the body and the voltage (or potential difference).

The damaging factor in electric shock is current flow. Current rather than voltage is the most important variable in establishing the criterion for shock intensity. Three factors that determine the severity of electrical shock are
1. Quantity of current flowing through the body
2. Path of current through the body
3. Duration of time that the current flows through the body.

The voltage necessary to produce the fatal current is dependent upon the resistance of the body, contact conditions, and the path through the body (Ref. 8).

The shock effects produced by a 60-Hz ac current or a dc current may be as follows (Ref. 8):
1. *0-1 mA ac, 0-4 mA dc.* Shock becomes perceptible. Normally harmless in itself at this magnitude
2. *1-4 mA ac, 4-15 mA dc.* Surprise—its primary effect—is an involuntary reflex action. The reflex action may cause an inadvertent motion that could lead to a loss of balance and a fall or a head injury or other injury worse than the shock itself.
3. *4-21 mA ac, 15-80 mA dc.* Very strong involuntary reflex action with consequent probability of indirect injury. In this current range the victim may not be able to let go of the conductor due to the clamping effect. This "let go" current varies among people but is close to 9 mA for men and 6 mA for women at 60 Hz ac.
4. *21-40 mA ac, 80-160 mA dc.* This intensity is adequate to cause an adult to lose control of affected muscles.
5. *40-100 mA ac, 160-300 mA dc.* Results in respiratory block. Currents in this range can be very painful and injurious. Prolonged contact may produce collapse, unconsciousness, and death due to paralysis of the respiratory muscles so that asphyxiation results. If the

respiratory muscles are paralyzed more than 3-4 min, the probability is that they will remain paralyzed and death is practically assured.

6. *Over 100 mA ac, Over 300 mA dc.* Currents of this magnitude that last 0.25 s or more can be almost immediately fatal. The heart loses its ability to contract in a coordinated beat; the individual muscle fibers twitch or fibrillate; blood circulation stops; and the heart itself, the brain, and other tissues stop receiving oxygen. This is referred to as ventricular fibrillation and is usually fatal unless immediate remedies are undertaken. Alternating currents are more dangerous than direct currents for causing ventricular fibrillation. The heart will rarely recover from ventricular fibrillation by itself but may be restarted by a strong, short-duration external shock. This countershock excites all the heart muscle fibers at once. They are quiescent for an instant; then, hopefully, the heart will resume its regular beat.

7. *2.5 A or Higher, ac or dc.* A current of this magnitude will clamp or stop the heart as long as current flows. The heart will usually start on its own once the current has been removed. The victim may be unconscious. Paralysis of respiratory functions may occur, and resuscitation is required within 3 or 4 min or brain damage or death will probably result. Alternating currents of this magnitude will also cause serious burns to the skin and internal organs. Burns on the skin will also decrease the resistance of the skin and cause even more damage if the current is not removed.

The physiological effects of a shock depend on the current path, current frequency, and duration. A relatively large current can pass from one leg to the other with only contact burns. The same current from arm to arm, or arm to leg, may clamp the heart and/or paralyze respiratory muscles. Alternating currents are more dangerous than direct currents; 18 V ac have been known to cause a fatality (Ref. 41), whereas direct currents require a higher voltage, over 100 V, to cause a fatality.

Alternating currents with frequencies of 20 to 100 Hz are the most hazardous, and 60 Hz is the frequency most likely to cause ventricular fibrillation. Generally, the higher the frequency, the less chance of ventricular fibrillation. Also, as the frequency increases, the currents travel closer to the surface of the conductor; this is known as skin effect. Currents at higher frequencies will tend to travel along the skin and less through internal organs and thus cause less internal damage.

When the resistance of the skin is lowered, the current flow for a given potential difference increases. When the skin is dry, skin resistance is high and a shock may only be mild. However, if the skin is not dry, the shock may be severe or even fatal. Most of the time skin is not completely dry because even minor perspiration will lower the resistance of the skin; consequently, the possibility of a severe shock is high.

A basic safety rule for electrical work should be that no work is performed on electrical equipment or circuits until the power to the equipment is turned off. The power should not only be turned off but locked out so that it cannot be accidently repowered by someone else. Access to electrical equipment should be restricted and interlocks provided to remove power if the access door or cover is opened. Interlocks, lockouts, and lockins were discussed in detail in par. 9-2.4.

A rule used by old-time electrical workers is never to use two hands to work on electrical circuits. The rationale is that inadvertent contact with live circuits will then be between fingers or from one arm to the foot and not through the heart. Unfortunately, most electrical work requires both hands.

Nearly all electrical equipment contains shock hazards. MIL-STD-454, Requirement 1, (Ref. 8) states that personnel should not come in contact with over 30 V. Some equipment has circuits that contain capacitors that store electrical charges at potentials much higher than 30 V; these capacitors can deliver severe shocks even with power removed from the circuit. When the power is removed, the capacitors remain charged unless the charge is bled off by some path to ground. A safe practice is to provide resistance grounds to deenergize the capacitor. The resistance should be high enough to allow the circuit to operate properly when powered and low enough to bleed off the charge within a few seconds after the power is removed from the circuit. MIL-STD-454, Requirement 1, (Ref. 8) requires capacitors to be automatically discharged if the circuit does not reduce to 30 V or less within 2 s after shutdown.

Another shock hazard is from defective insulation on conductors. Insulation can be defective due to deterioration, damage, or inadvertent removal. Although the insulation will appear to be adequate, it may actually be conductive enough to cause a shock hazard. There are a number of reasons for breakdown of insulation, i.e.,

1. *Elevated Temperatures.* May cause a slow but gradual breakdown of some polymers. A flow of current always results in an increase in temperature of the conductor and its insulation.

2. *Cold Temperatures.* Insulation is usually more susceptible to damage if it is cold because it may then become more brittle and may crack and break more easily.

3. *Moisture and Humidity.* May cause a deterioration of insulation and may reduce its insulating capability directly by absorption of moisture into the insulator.

4. *Oxidation.* Will have an effect on insulators. Ozone causes more deterioration than oxygen because of its greater reactivity. Large quantities of ozone are created by electrical arcs or coronas, which occur in motors, generators, and other electrical equipment.

5. *Radiation.* Will degrade the properties of insula-

tion. The insulation is actually degraded by the reaction products created by ultraviolet or nuclear radiation. Other chemicals can directly damage and degrade insulation.

6. *Mechanical Damage.* Can result from abrasion, cutting, vibration, flexing, crimping, or being crushed by another object.

7. *High Voltages.* May cause sparking or corona effects, which can puncture holes in the insulation, create reactive products, and generally reduce the resistivity of the insulation to voltages.

8. *Biological Factors.* Can cause insulation problems. Animals and insects may eat, weaken, or entirely destroy the insulation.

9. *Pressure.* Changes in pressure will affect insulation. A vacuum will cause an outgassing of the volatile components of the insulation and result in the release of gas, dimensional changes, and reduction of its resistance to flexing and mechanical abuse.

10-14.2 IGNITION OF COMBUSTIBLE MATERIALS

Combustibles are usually ignited electrically by a spark or arc. A spark is created when electrons flow across an opening gap from one electrode to another—usually by contact breaker points or a relay—through the intervening medium when a circuit is opened. An arc occurs between a bare conductor and a nearby bare conductor or ground. As a charge builds on the electrodes, the air (or other gas) near the electrodes begins to ionize and to reduce the dielectric strength of the air. If the electric field is strong enough, ionization will continue across the entire gap until there is a complete conductive path between the conductors or the conductor and ground, and an arc flows. If the discharge is energetic enough and a flammable mixture of gas and air is present, the arc or spark will heat the air and cause ignition of the flammable mixture. To prevent electrical ignition, the sources must be removed. Electrical equipment should not be situated in areas where flammable mixtures might exist.

It is possible for a surface to be electrically heated to a temperature at which the surface ignites a flammable mixture. (See par. 10-14.3.) To do so, however, the surface must be extremely hot, which may require the expenditure of a large amount of energy. For this reason the hot surface is not as prevalent an ignition source as an arc or spark, which usually involves comparatively little energy concentrated and discharged in a small volume of flammable mixture.

10-14.3 HEATING AND OVERHEATING

Whenever there is a flow of current in a conductor, heat is always produced and the temperature of the conductor increases. The amount of heat depends upon the amount and frequency of the current and the properties of the conductor. In general, the higher the resistance of the conductor, the greater the power loss and the higher the temperature of the conductor.

A principal result of electrical overheating is accidental fires. Overheating can raise the temperature of a flammable mixture to a point at which it can be readily ignited by another source or to a point at which it does ignite. Overheating can cause other materials to char or burn and can cause vaporization of liquid fuels to create flammable mixtures with air. Overheating can also result in damage to electrical equipment. The overheating can raise the temperature of the equipment high enough to induce failures or, sometimes, to ignite the equipment. If the heating is so rapid that it cannot be dissipated quickly, a violent explosion may result.

10-14.4 INADVERTENT ACTIVATION

Equipment that is activated or energized unexpectedly, depending upon the type of equipment, can cause serious injury or death. Shock hazards are possible if equipment is activated unexpectedly, as previously discussed in par. 10-14.1. Inadvertent activation can usually be prevented by using lockouts and interlocks.

Quite often, motors and other rotating equipment are activated automatically. Motors may drive compressors, generators, refrigeration units, and other equipment that is energized when the pressure drops below a certain point, the temperature increases or decreases beyond a preset value, or voltage changes require an on-line generator. These activations may come unexpectedly and could cause injury to a person in a vulnerable position if the equipment is not properly locked out prior to adjustment, maintenance, or inspection.

10-14.5 FAILURE TO OPERATE AS REQUIRED

When equipment fails to operate, it is generally in a safe, passive condition. Normally this will not result in a hazardous situation, but in some instances a hazardous condition could result. For example, a weapon with electronic firing could fail and leave the weapon in an unsafe condition. A missile on a launcher that failed to fire on command must be regarded as "hangfire" ammunition until either fired or safed in an appropriate manner. If an electronic warning device fails, it may not warn of a hazardous condition. An electronic circuit may fail to operate as required and cause loss of control of a vehicle, a missile, or other weapon, which could result in injuries or even fatalities.

In some cases, a series of events must occur in a prescribed sequence to accomplish a final action, and a failure at any step may cause the next step to become a hazardous situation. For example, in an Army missile system, the resupply of missiles into the storage magazine and the loading of missiles on the launcher are critical

operations. The sequencing of the functioning of doors, missile-holding devices, and the turret holding the launchers must be exactly right for each step of each separate operating mode—i.e., resupply, loading, tracking, and firing. If the sequencing or completion of one operation is incomplete and that malfunction is not detected because of failed circuits, the continued operation of the system could be hazardous. Accordingly, it is important to insure that a sequence of events does not result in a hazardous situation if one or more steps fail to occur.

10-14.6 ELECTRICAL EXPLOSIONS

Electrical explosions are usually caused by excessive currents through electrical devices. The excessive current causes rapid thermal heating and builds up pressures that usually rupture the electrical device. The effect is used beneficially in exploding bridgewire (EBW) initiators in which a comparatively massive current is forced by a high voltage through a small conductor that is heated so rapidly it vaporizes in an explosion. High-voltage and high-current short circuits can create the same effect accidentally if the conductor offers high resistance.

A fully charged battery can explode if shorted so that high currents cause rapid heating. Internal pressures build up faster than they can be relieved through the vents. Electrolytic capacitors can explode violently if they are installed with reverse polarity and energized or if they are installed correctly and energized at a greater-than-design potential.

Large transformers (and some capacitors) contain a liquid, usually a silicone or other type oil. These devices can overheat—especially if the oil contains a contaminant such as water—and explode; the explosion sends extremely hot oil over a large area. Under the right circumstances, even resistors may explode with unexpected violence. For example, in a tuned RF amplifier, a filter may have a high impedance at other frequencies. If the input signal changes enough, the current through the filter could be adequate to explode a resistor with violence.

As discussed in par. 10-14.2, arcs and sparks can cause other nonelectrical explosions (Refs. 75 and 76). In a flammable, or explosive, atmosphere, an arc or spark can provide the necessary energy to ignite the explosive mixture.

10-14.7 STATIC ELECTRICITY

Static electricity is a phenomenon that has been well-known and documented for years. Only recently, however, has it been recognized as a major cause of industrial accidents. All of us have experienced the annoying shock that results from walking across a rug on a dry day and touching a grounded object such as a water faucet. This shock is caused by a static electrical charge that builds up

on the body due to the rubbing of one's shoes on the dry carpet. What is not immediately recognized is that this static charge can build up to a dangerous level just by the movement of clothing, by air blowing through an air-conditioning duct, by the sloshing of solvents in a glass beaker, or by the flow of organic hydrocarbons through a hose. Investigations have shown that uncontrolled static electricity can cause serious hazards to plants and operating personnel and to product quality and rate of production. Fires and explosions can result from the electrostatic ignition of flammable vapors that arise from the use of industrial solvents and other flammable mixtures. Personnel can be caught in the moving parts of machines by the involuntary muscular response resulting from high-voltage sparks and the accompanying electric shocks (Ref. 77). To emphasize the potential for injury or damage, consider the illustration in the paragraph that follows.

It has been shown that the charge buildup on a human body may be as high as 50,000 V (Ref. 78). This voltage is far in excess of that required to jump a spark across a small air gap to an object of lesser potential. The energy available in such a spark can be calculated and compared with ignition energies of various solvent vapors and other explosive mixtures. Consider the human body as a capacitor with a capacitance C of 10^{-12} F. The stored energy E can then be calculated by

$$E = CV^2/2, \text{ J} \qquad (10\text{-}6)$$

where
V = body potential, V.

Since in this case $V = 5 \times 10^4$ V,

$$E = 10^{-12}(5 \times 10^4)^2/2 = 0.01 \text{ J}.$$

Compare this energy of 0.01 J with the ignition energies shown in Table 10-44 (Ref. 79); it is evident that a static spark could easily ignite a number of solvent vapors.

The generation of static electricity usually involves two nonconducting surfaces, initially in contact, that are suddenly separated. The two materials or phases in initial contact may be two solids, two immiscible liquids, a solid and a liquid, a solid and a vapor or gas, or a liquid and a vapor or gas. The important thing to remember is that whenever there is contact and separation of phases, a charge is developed that could be disastrous. To determine the theoretical potential difference that could result from the separation of two nonconducting surfaces, consider the two nonconductors initially no closer than the normal distance between atoms or molecules, i.e., 10^{-7} mm, at which the potential difference was a modest 0.01 V. If the two materials were separated perfectly, i.e., with no electrons flowing back across the junction, the potential

TABLE 10-44. MINIMUM IGNITION ENERGIES REQUIRED TO EXPLODE VARIOUS LIQUIDS AND GASES (Ref. 79)

	Explosive Range, % concentration by volume	Minimum Ignition Energy, J
Acetone	2.6 -12.8	0.0006
Benzene	1.4 - 7.1	0.0005
Butane	1.9 - 8.5	0.00064
Carbon Disulphide	1.25-50.0	0.00015
Cyclopropane	2.4 -10.4	0.00018
Ether (Diethyl)	1.85-36.5	0.00045
Alcohol (Ethyl)	3.3 -19.0	0.00065
Gasoline	1.4 - 7.6	0.001
Hydrogen	4.0 -75.0	0.00002
Methane	5.3 -15.0	0.00096
Methyl Alcohol	6.7 -36.0	0.0005
Propane	2.2 - 9.5	0.00036

Reference: Federal Bureau of Mines

Reprinted with permission. Copyright © by R. L. Mondano.

difference would increase as the distance between the materials increases. Thus when only 10 mm apart, the potential difference between the surfaces would be 1,000,000 V. Fortunately, the actual voltage is much less because some of the electrons flow back through contact. Also the intense electric field produced ionizes the surrounding atmosphere and, thereby, permits the dissipation of much of the charge. The residual charge, however, could still ignite flammable mixtures (Ref. 59) or cause an explosion.

The hazards from static electricity are the same as those from any other electrical arc or spark. A static charge, however, generally occurs only once unless the static charge generator is in continuous operation. In this case, the static discharges may be continual but not continuous as is the arc supplied by a steady, high-voltage current. Continual electric static discharges have been known to burn pits in the surfaces of bearings that act as grounds. A static discharge is also capable of destroying transistor junctions in integrated circuits and thus render the circuit inoperative (Ref. 77). The voltage required to destroy an integrated circuit is about 50-100 V, depending on the circuit. It is important to recognize that voltages of this magnitude can be generated in the packing and unpacking of microchips unless proper precautions are taken relative to packaging material and handling.

As previously discussed, static electricity can be generated by two nonconducting materials in contact with each other, e.g., a liquid and a solid. Such is the case when liquids move through a pipe or a hose. If the liquids are flammable, under certain conditions they can boot-strap themselves to self-ignition or explosion. The potential for such an ignition can be identified—and subsequently eliminated—by a careful examination of all the factors involved. An excellent example of the hazard—due to static electricity—arising from the movement of a flammable liquid is quoted from Ref. 78:

"Consider this incident. A fire started when an operator was drawing a bucket of toluene from a tank that was an integral part of process equipment. He had placed a metal bucket with a wire bail and plastic handle under a globe valve that was two feet downstream from an in-line filter. He had opened the valve to draw the toluene. In a few seconds, the toluene ignited."

"During the investigation of the accident it was concluded that the operator had opened the valve, withdrawn his hands, and was simply looking at the bucket when ignition occurred. In the consideration of the ignition source, electrostatics were considered to be the most probable; however, discharge from the operator was ruled out since he was not near the bucket. 'I was just standing there looking at it when it caught fire,' he said. Also ruled out as a source was the possibility of a charge having been generated on the bucket prior to the operation. The mechanism of a streaming current [i.e., the flow of electricity produced by the capture or loss of electrons by a flowing fluid] was then considered.

"The conductivity of the sample of toluene taken from

the process was measured in the laboratory at 2.9×10^{-11} mho/cm. The literature value for the [dynamic] viscosity of toluene is 5.9 cps [centipoise], and its dielectric constant is given as 2.4. Knowing from the process that a pressure drop of 35 psi occurs in the last two feet of [a one-inch] pipe (i.e., from the filter to the end of the pipe), and knowing the capacitance of the bucket as being of the order of 20 pF, and remembering that ignition occurred approximately 10 seconds after the valve was opened, a mechanism of the charge being generated by the flowing of the toluene and subsequent discharge from the bucket can be made quantitative as follows:

"If it is postulated that the charge was generated by the flowing of the toluene through the pipe, the question arises as to whether or not sufficient energy could be generated to result in a discharge that could ignite toluene.

"First, streaming current I_s is calculated from the streaming current equation...

$$I_s = \frac{A\epsilon\epsilon_o\zeta\Delta P}{\mu L}, \text{A} \qquad (10\text{-}7)$$

where

A = area of the pipe = $3.14 \ (2.54)^2/4 \ \text{cm}^2$

ϵ = relative dielectric constant for toluene = 2.4, dimensionless

ϵ_o = absolute dielectric constant (permittivity) = $8.85 \times 10^{-14} \ \text{s/ohm·cm}$

ζ = zeta potential, i.e., potential difference across a double layer in a liquid medium = 0.1 V

ΔP = pressure drop = $35 \times 6.89 \times 10^4 \ \text{dyn/cm}^2$

L = pipe length = $2 \times 12 \times 2.54$ cm

μ = dynamic viscosity of toluene = 0.059 dyn·s/cm^2 = 5.9 centipoise.

[Substitution of these parameter values into Eq. 10-7 gives]

$$I_s = 7.2 \times 10^{-8} \ \text{A}.$$

"If this current flows for 10 s and is stored on the bucket, which has a capacitance of approximately 20 pF, the energy J is given by

$$J = \frac{Q^2}{2C} = \frac{(I_s t)^2}{2C}, \text{J} \qquad (10\text{-}8)$$

where

Q = charge, coulombs

C = capacitance = 20×10^{-12} F

t = time = 10 s.

[Substitution of the parameter values into Eq. 10-8 gives

$$J = \frac{(7.2 \times 10^{-8} \times 10)^2}{2 \times 20 \times 10^{-12}} = 0.013 \ \text{J}.]$$

"This is, by order of magnitude, more energy than that required for ignition of compounds of this type....[See Table 10-44.]

"The charge that has been generated by the streaming current I_s initially resides in the toluene. In this instance, the charge is quickly transferred to the exterior of the bucket, as shown by the relaxation time t_r of the charge from the body of the toluene calculated by the relaxation equation

$$t_r = \epsilon\epsilon_o/\gamma \qquad (10\text{-}9)$$

where

γ = conductivity = 2.9×10^{-11} mho·cm."

Substitution of the parameter values into Eq. 10-9 gives

$$t_r = \frac{2.4 \times 8.85 \times 10^{-14}}{2.9 \times 10^{-11}} = 0.007 \ \text{s}.$$

"In other instances, toluene may have conductivities of $\gamma \le 10^{-14}$, in which case a space charge would remain on the body of the toluene for much longer periods. In such a case a different mechanism prevails, but a hazardous situation would still exist.

"Discharge could take place to any convenient ground (around the plastic handle) if the voltage is high enough. In this situation the voltage can be determined from the energy relation" [Eq. 10-8 since $Q = CV$]

$$J = \frac{CV^2}{2}, \text{J}$$

$$V = \frac{2J}{C}, \text{V}$$

$$= 2 \times 0.013/(20 \times 10^{-12})$$

i.e., $V = 36,000$ V.

"This compares with the requirement of 30,000 volts to discharge between 2 cm electrodes at a separation of 1.8 cm....Thus, ample potential was present to support the bootstrap scenario." (Ref. 78)

This example should give the designer some insight as to where and how streaming currents can lead to fires and what to look for in a process to determine whether precautions are necessary. The values of the parameters

used in the previous discussion must be of the right combination to result in a hazardous situation; however, the designer or operator must be especially concerned when flammable liquids of low conductivity are used in processes with high flow rates and large pressure drops, e.g., the transferring or fueling operations for vehicles or missiles (Ref. 78).

Filling a fuel tank, therefore, can be a hazardous operation. The possibility of sparking between charged fuel in a tank and the walls or roof of the tank is also enhanced by the charges on droplets in the air space. The hazard increases with the rate of flow as indicated by the streaming current equation, Eq. 10-7. A metallic object on the surface of the fuel, such as a float, will aggravate the situation even more by acting as one plate of a condenser and collecting electrical charge from the fuel. The sides and roof of the tank act as the other plate of the condenser. Consequently, when the potential from the charge is great enough, a spark may occur. Since the atmosphere in the tank is occupied with fuel vapor containing ionized particles, the potential required to produce a spark is much less than that required in dry air. Methods have been employed to neutralize or reduce the charge without creating a spark or causing a hazard in the tank. One method is to insure that all conductive parts in fuel systems are electrically bonded. Fuel additives to prevent charge buildup is another possible solution.

Other hazards resulting from static electricity in fluids include

1. Fires resulting from sparks generated by fuels or other liquid chemicals flowing through fill lines

2. Explosions and destruction of fuel tanks when water used to hose down the tanks generates streaming currents that produce charged potentials and consequent sparks that may ignite vapors in the tanks

3. Aircraft flying through air masses containing charged particles accumulate charges on the aircraft structure. Unless the resulting static discharge currents are finely divided by means of static discharge devices, those discharges cause interference with communications and other electronic equipment.

4. Charges, generated by the rotating blades of helicopters, that produce violent shocks to personnel who touch an ungrounded helicopter or a conducting line attached to it

5. Spray processes, involving flammable materials such as paint, that cause charges to build up as the droplets leave the spray nozzle, pass through the air, and are deposited on the surface being painted. When an opportunity for a discharge of the accumulated charge occurs, the resultant spark can cause an explosion and fire in the flammable paint mist.

The most massive natural discharge of static electricity involving high potentials and high current is lightning (Ref. 80). Lightning follows the path of least resistance to

earth. The least resistant path may be a desirable one, such as lightning rods, lightning arrestors, and other grounds, or it may be an undesirable one, such as equipment or personnel. The hazards to a person from a lightning strike are usually burns or immediate death from electrocution. Equipment damage is usually severe: Circuits are destroyed, or the equipment is damaged by fire or explosion. Electrical equipment can also be damaged by currents induced in conductors by a lightning discharge.

10-14.8 TOLERANCE AND SAFE EXPOSURE LIMITS

The effects on persons of various current levels have been indicated in par. 10-14.1. Currents of 1 mA may surprise but will not injure a person. Currents of 5 mA or more will cause injury; therefore, some specifications, e.g., MIL-T-28800 (Ref. 81), indicate that protection must be provided against currents in excess of that amount.

Because current is far more difficult to measure than voltage, other documents, e.g., MIL-STD-454 (Ref. 8), have established 30 V as the level at which protection must begin. Thirty volts is considered the potential at which 5 mA will flow through the resistance offered by the body of a normal human being. However, under certain conditions, the resistance of the body will be far less than normal; consequently, far higher currents will flow. Such conditions include situations in which a person is perspiring heavily; is standing in or is otherwise immersed in water; or is injured, wounded, or undergoing an operation, in which case the skin is not intact and current can pass readily through the more highly conductive internal tissues.

10-14.9 POTENTIAL HAZARD SOURCES

Twelve- or 24-V systems will generally provide little danger to personnel from shock hazards unless, as indicated previously, a person is wounded so that his skin resistance is substantially reduced. However, even 12- or 24-V systems can generate other hazards. A very common example of spark generation occurs with 12-V batteries when connections to terminals are made or broken with battery cables or the alligator jaws of jumper cables. The sparks generated then are adequate to ignite hydrogen or other flammable mixtures that might be present.

Other low-voltage systems might carry large currents that can generate large amounts of heat, which result in hot surfaces on which persons can be burned or combustible material ignited. This heat can also cause degradation and failure of other components. Further, low-voltage systems sometimes contain large-capacity capacitors charged to high energy levels. When shorted, these capacitors become very low-resistance energy sources and increase the low-voltage hazard. Very low-voltage

batteries inadvertently have been shorted; the results are a fast thermal reaction, overpressure, and consequent battery explosion (case rupturing). Thus, low-voltage systems are not intrinsically safe simply because they operate at low voltages. *All* electrical systems should be considered sources of potential hazards.

10-14.10 DESIGN CONTROL TECHNIQUES

Most of the criteria for design control of electrical hazards in Army systems are stipulated in Requirement 1, MIL-STD-454 (Ref. 8). Additional requirements, such as for minimizing problems of inadvertent activation of electroexplosive devices, are contained in MIL-STD-1512 (Ref. 82). In addition, other techniques such as those stated in the paragraphs that follow should be used.

Insulation should be guarded to prevent degradation and the resulting reduction of protection against short circuits and shock. The insulation selected should be suitable for the environmental conditions to be encountered. Electrical equipment should be cooled or ventilated to remove excess heat. Moisture in vapor and liquid form should be considered when designing a system, and vapor protective coatings or enclosures and/or drain holes should be provided. Radiation should be contained and not allowed to reach and damage insulation. (See par. 10-8.)

Mechanical damage to electrical insulation should be a design consideration. One of the most frequent reasons for insulation damage results from neglecting the effects of vibration. Another source of mechanical damage is crew movement in both ground and air vehicles, including normal entry into and exit from the vehicle. Accordingly, physical protection of electrical wire bundles and electrical equipment against crew-induced mechanical damage must be an electrical installation design feature.

The primary precaution to be taken for protection against electrical shock is adequate grounding. Grounding can be designed and installed into a system, or it can occur accidentally. An accidental ground may be provided by an operator's body and could cause a fatality. If a permanent path is provided for the return of electrical current so that it will pass through the designed ground and not the body, the shock hazard is reduced. MIL-STD-454 (Ref. 8), MIL-STD-188/124 (Ref. 83), and Refs. 84 and 85 contain guidance for those who wish to study the subject of grounding in detail.

Grounding (and bonding) in Army equipment is a simple design procedure when one understands the objective, i.e., provide a "safe" path for current return from any electrical fault. A common misconception in the design application of grounding principles is that if all the conductive enclosures are grounded, i.e., connected to an earth ground, then the equipment is satisfactorily grounded. This concept is not necessarily true. If the paths to ground and the return to the energy source have

different impedances, then current may flow through several "returns" to the energy source. This situation is unsafe for both personnel and equipment.

Before determining the correct grounding procedure, it is necessary to clarify the terms and their meanings as used in the National Electrical Code (Ref. 86), i.e.,

1. *Grounding (Earthing) Electrode Conductor.* This conductor connects equipment, or the system, or both to their surroundings, i.e., the earth, a conductive building, and/or conductive conduits.

2. *Equipment-Bonding Conductor.* This conductor connects conductive enclosures or equipment frames together but not necessarily to ground.

3. *System-Bonding Jumper.* This conductor connects the system conductor to an equipment-bonding conductor but not necessarily to ground.

When these three conductors are installed as shown in Fig. 10-39 (Ref. 85), the system is electrically safe *provided* the ground-loop impedance is low (0.25 ohm or less) and maintained low. Fig. 10-39 is simpler than most examples of Army equipment that will be encountered by the designer. The complex situations may involve equipment in hazardous locations (explosive atmospheres or materials), sensitive equipment (to electromagnetic or static influence), equipment with many enclosures or separate units within an enclosure, and multiple phase and ungrounded systems. To design bonding and grounding properly for these conditions, the designer should study the ample discussions and provisions of MIL-B-5087 (Ref. 84).

In addition, the following guidelines implement the principles of correct electrical design for protection of personnel from electric shock (Ref. 87):

1. *Interlocks.* Provide a means to remove power whenever a cover or other barrier to electrical equipment has been removed.

2. *Isolation.* Enclose and keep high-voltage equipment away from points where personnel may accidentally contact it.

3. *Marking.* Provide warning labels or other notices to warn of hazards, or provide instructions or procedures to minimize the hazard.

4. *Warning Devices.* Provide lights, audible warnings, or visible indicators to alert personnel that circuits have been activated.

5. *Ground Fault Circuit Interrupters (GFCI).* This is a device that monitors current flow from the supply and to the return. If there is a difference—as there would be if current were flowing through a person to ground—the GFCI senses the difference (as little as 5 mA), and the supply of current is very rapidly cut off. The NEC now requires the use of GFCIs generally in wet areas where 120-V, single-phase lethal voltages are present. Bathrooms, marinas, construction sites, and other places where portable appliances and tools are powered through
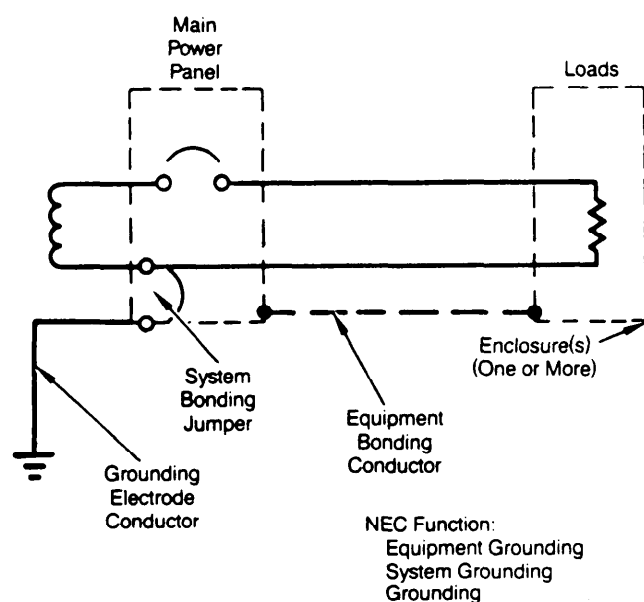
Adapted from January 1978 *Professional Safety*, official publication of the American Society of Safety Engineers.

Figure 10-39. NEC Grounding Terminology and Installation (Ref. 86)

drop cords are common locations where GFCIs may be required. GFCIs can be used to provide safe electrical operating conditions for similar Army situations.

6. *Barriers*. Provide barriers or guards for all electrical terminals or exposed conductors whose voltages with reference to ground are 30 V or more to prevent accidental finger contact.

When equipment must be located where flammable mixtures might exist, other precautions should be taken. It is advisable in all circumstances to avoid locating equipment that can generate arcs or sparks in atmospheres that might become flammable. Table 10-45 lists the minimum spark ignition energies of some flammable vapors and illustrates how little energy is required. If equipment must be located in areas where flammable vapor is a possible environment, the electrical equipment can be sealed into a container that is filled with a dielectric liquid, inert gas, or a solid. If the filler is a solid, the electrical equipment may be (1) molded into it or (2) sealed into a hollow container. These two methods of enclosing equipment in a solid are known as embedment and encapsulation, respectively. Hermetic sealing with an inert gas usually has better thermal properties than solid encapsulating because the solids used for encapsulating are generally poor conductors of heat. Liquids have absorptive thermal properties and superior dielectric strengths that help to prevent arcing or sparking.

Another means to prevent ignition of a flammable mixture by an arc or spark is to use explosion-proof

equipment and lines. Although it would appear to be a contradiction in terms, an explosion may occur inside an explosion-proof device when flammable gas leaks into an enclosing case and is ignited by a spark or arc. Leakage, for example, may occur through joints necessary to connect a conduit with equipment. Also a rotating shaft must have some tolerance or clearance; gases can enter if the seal is not airtight. To meet the NEC definition of "explosion proof", equipment must be "enclosed in a case which is capable of withstanding an explosion of a specified gas or vapor which may occur within it, and of preventing the ignition of the specified gas or vapor surrounding the enclosure by sparks, flashes or explosion of the gas or vapor within, and it must operate at such an external temperature that a surrounding flammable atmosphere will not be ignited thereby." (Ref. 76).

Explosion-proof equipment requires special care. The basic consideration is that it must be designed for the specific gas or vapor that is expected since flash points, explosion pressures, and ignition temperatures of explosive fuels vary. Design of containers should be specified with cognizance of the principles of flame-tight joints and case pressure requirements. Flame will not carry through a passage whose length is great in proportion to its width or diameter. Flame-tight joints rely upon this principle, which permits gases to cool below ignition temperature before exiting the case. If screwed fittings are used, at least five full, finely machined threads must be engaged, and they should be tightened within the tolerance prescribed to prevent loosening by vibration. If lighting fixtures are required, each explosion-proof fixture should be marked to indicate the maximum wattage lamp to be used; this maximum should never be exceeded.

An alternative to approved explosion-proof equipment may be the use of pressurized systems for electrical equipment in hazardous locations. Either air or inert gas pressurized above the ambient atmospheric pressure prevents entrance of flammable gas into the enclosure in which electrical equipment might act as a source of ignition. If clean air is used, a positive head pressure of at least 25 Pa (2.54 mm (0.1 in.) of water) equivalent pressure should be maintained inside the equipment housing. The clean air purges the system of contaminant gas. If an inert gas is used to pressurize the equipment enclosure, it has the added advantage of removing the oxidizer required by a flammable substance to support combustion. Whether inert gas or air is used, a pressure switch interlock for system power will keep the system from being energized prior to the buildup of pressure in the enclosure or in case pressurization fails. Pressurization is a desirable approach for the operation of some types of electrical equipment at high altitudes. The pressurized equipment enclosure presents a more normal atmospheric pressure that will prevent the coronas and arcing that would otherwise occur at high altitude and low air

TABLE 10-45. OBSERVED PHYSIOLOGICAL EFFECTS OF IMPACT (Ref. 90)

Effects	Impact Force	Responses
Bradycardia	$5-15+G_x$	Slowing of heart for at least 5 beats
	$15-30\pm G_x$	Slowing of heart rate immediately following impact
	$9-12+G_1$	At higher accelerations slowing is increased. 1.6 mg atropine eliminates slowing, indicating relationship to vagal reflex
Shock	$>15\pm G_x$, 500 $G's$	Brief disorientation, drop in blood pressure to 90/60 mm Hg 15-30 s postimpact, ECG nodal rhythm
	$12+G_1$	Faint, pallor
Muscular	$>26-G_x$, 850 $G's$, 0.002 s*	Chest pains, aches in back and neck muscles, stiff neck 1-3 days
Skeletal	$>16+G_z$, 1160 $G's$	Anterior lip vertebral compression fracture; most observed injury L1-T7
	$>16-G_x$, 0.01-.10 s	Fracture of lumbar vertebrae
	to $83+G_x$, 3800 $G's$, .04 s	None
Neurological	$\pm 15-G_x$	Increased deep tendon reflexes
	$>20-G_x$, 400+800 G s	Appear stunned 10-15 s at 20 G peak accelerations. Euphoria, hand tremor, decreased coordination, loquacity, increased muscle tone, gross involuntary movements in head, arms, trunk
	25 G	Deep tendon reflexes absent for several seconds, then hyperactive for about 1 min
	>25 $G-G_x$, 1000 $G's$	Abnormally slow EEG wave patterns observed for several min postimpact
Hematological	$20-G_x$, 400+800 G s	Blood thrombocytes reduced 1 h postimpact. A week later thrombocyte count higher than control value
Psychological	10 to $-G_x$	Kohn symbol arrangement test shows distinctive changes, increasing with force level
General Stress	$>20+G_x$	Chemical changes in adrenal blood; alterations in adrenal gland activity
		17-OHCS excretion levels increase significantly and are related to anxiety and CNS stimulation of adrenocortical secretion

*To be interpreted as "$26-G$, for 0.002 s with a calculated rate of onset of 850 $G's$". Here G is magnitude only.

pressure. In addition, the pressurization also will keep flammable vapors and contaminants out of the equipment enclosures.

Problems of overheating may be overcome by various protective devices. Fuses and circuit breakers are designed to open when specific limits have been exceeded and thus remove power from the device they are protecting. A number of different types of fuses and thermal circuit breakers are available. The type to choose depends upon the currents involved, the type and duration of the load, probable short circuit characteristics, ambient temperatures, and the type or characteristics of the operation involving a human operator. Trip-free circuit breakers that cannot be reset as long as a fault remains in the system should be used if momentary reset attempts could damage the shorted equipment.

Temperature sensors can be employed to monitor the temperature of electrical equipment and shut it off when a preset temperature is exceeded. This type of protection can be used even when the source of heat is external to the electrical equipment. Positive air flow, or liquid flow cooling, can also be used in conjunction with heat sinks or other heat dissipation devices. In equipment that generates heat during normal operation, cooling will lengthen the service life (improve reliability) as well as guard against hazards from overheating.

Equipment should be protected against inadvertent activation caused by accidently pressing a button,

bumping a switch, or other action. Preventive measures include interlocks, recessed buttons, switches with guards, and dual- and series-wired switches or buttons located far enough apart to preclude activation of both by one person.

Occasionally, inadvertent activation of equipment may result from mislabeling a switch or control or from omitting the label. The solution is to insure that all switches and controls are labeled correctly. If the control operates dangerous equipment, moving equipment, or high-voltage equipment, a warning label should be used.

Sometimes inadvertent activation may be caused by failures of other components of electrical systems. Through suitable subsystem analyses described in Chapter 5, designers and analysts can determine under what circumstances inadvertent activations could occur through errors, failures, or adverse environmental conditions. When the consequences of an inadvertent activation could be serious, such analyses are mandatory.

Preventive measures against safety-critical failures include redundant systems, warning devices, components with very low failure rates, and alternative methods to accomplish the failed events. If a particular instrument is critical, a redundant instrument should be added as a separate system. If a power failure could cause a hazardous situation, an alternate backup system should be available. In addition, if a particular circuit is critical, it should be fabricated from high-reliability parts to avoid a failure. These preventive measures apply to all electric equipment but are critical when a failure to operate creates or sets up a hazardous condition.

Prevention of static electricity hazards can be accomplished in two ways: (1) by preventing the buildup of accumulated charges and (2) by draining off, or safely neutralizing, the accumulated charges. There are a number of methods for preventing the buildup of charges. The simplest and best method is to select electrically (charge) conducting materials that do not generate or store static charges. If the problem is static charges generated by personnel, such as maintenance personnel working on sensitive circuits, the use of grounding devices and the appropriate clothing can prevent the generation of static charges. Cotton clothing should be worn, instead of wool, nylon, or other synthetics. Surfaces can be sprayed with coatings to make them conductive so that static charges cannot accumulate or will drain off quickly. Suitable bonds and grounds provide an effective path for dissipating accumulated static charges. These bonding and grounding techniques also help to protect the equipment and personnel near the equipment in the event of a lightning strike. (Ref. 84 is a complete treatise on this subject.) Other methods for dissipating charges are grounding bars on doors leading to hazardous areas and ground-stats for persons to wear.

There are four types of electrostatic devices for neutralizing accumulated charges, i.e.,

1. *Radioactive Neutralizers.* This method uses a radioactive source, such as radium or polonium, that emits positively charged alpha particles. The emitted positive charge neutralizes the negative charges on the material being processed. Radioactive sources are hazardous, however, and must be used with caution. See par. 10-8 for information on radiation hazards.

2. *High-Voltage Neutralizers.* This method (Ref. 88) produces a very high potential in the air near the surface being treated, which results in the ionization of the air. The positive ions resulting from this ionization combine with the electrons of the charged material and thus neutralize the static charge. The high voltage associated with this type of neutralizer presents an electrical shock hazard. (See par. 10-14.)

3. *Induction Neutralizers.* This system operates by producing potentials of polarity opposite to that of the material charged. Induction neutralizers can be used where high-voltage neutralizers are impractical due to size, safety, operational considerations, or other limitations.

4. *Humidification.* Increased humidification permits a rapid interchange and neutralization of charges so that they will not accumulate or, if accumulated, will dissipate quickly. In humidities above 65%, the charge is able to leak off instead of accumulating due to the conductive film created by the moisture on the surface of normally nonconductive material. This type of static charge prevention is usable when the environment can be controlled and the addition of moisture does not have a detrimental effect on other equipment.

Grounding electrical equipment is an effective method for preventing damage from lightning from both direct discharges and induced charges (Ref. 79). Overload protection is also used to prevent the large charges induced by lightning from damaging circuits. Lightning protection for Army equipment should be a design consideration from the beginning of an acquisition program (Ref. 84). The general characteristics of good lightning protection for mobile equipment include

1. Providing strong electrically conductive enclosures for all electronic units

2. Observing good design practices for bonding all units of equipment and their installation in the vehicle

3. Routing hard wiring so that electric and magnetic fields caused by currents in lightning discharges will not "generate" high voltages or currents in them by induction. (It may be necessary to shield wiring runs for better protection.)

4. Selecting materials that are incombustible since lightning strikes will most often cause ignition of any combustible material located near points heated by the large current flows.

Since the type of protection from lightning suggested here can only be provided by basic design techniques, it is

obvious that these requirements must be considered from the start of any acquisition program.

10-14.11 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

These following criteria are excerpted from MIL-STD-454 (Ref. 8), MIL-B-5087 (Ref. 84), and other sources of good electrical design practice:

1. The design will incorporate methods to protect personnel from accidental contact with voltages in excess of 30 V rms or dc during normal operation of a complete equipment.

2. Controls will be designed and located to prevent inadvertent activation of equipment that could cause injury or damage.

3. Means will be provided to cut off power while installing, replacing, or interchanging a complete equipment, subsystem, or any other item thereof.

4. A readily accessible main power ON-OFF switch will be located on the equipment and will be clearly labeled as to its function. The power input side of the switch and the incoming power line connections will be given physical protection against accidental contact.

5. The equipment will not cause ignition of an ambient explosive-gaseous mixture with air when operating in such an atmosphere.

6. The design and construction of the equipment will insure that all external parts, surfaces, and shields—exclusive of antenna and transmission line terminals—are at ground potential at all times during normal operation.

7. The design will include consideration of ground faults and voltage limits established on a basis of hazardous location.

8. Any external or interconnecting cable, where a ground is part of the circuit, will carry a ground wire in the cable terminal terminated at both ends in the same manner as the other conductors.

9. In no case, except with coaxial cables, will the shield be depended upon for a current-carrying ground connection.

10. Antenna and transmission line terminals will be at ground potential except for radio frequency energy on their external surfaces.

11. Plugs and convenience outlets for use with metal-cased portable tools and equipment will have provisions for automatically grounding the metal frame or case of the tool or equipment when the plug is mated with the receptacle.

12. Control shafts and bushings will be grounded unless the control knob or lever is insulated from the shaft.

13. All electrical and electronic units or components that produce electromagnetic energy will be equipped with a continuous low-impedance path (bonding) from the equipment enclosure to the structure. Test will

demonstrate that the proposed bonding method results in a dc impedance of less than 2.5 milliohms from enclosure to structure. The bond from the equipment enclosure to the mounting plate furnished with the equipment will also comply with these requirements except that suitable jumpers may be used across any vibration isolators.

14. When radio interference filters are used in the power input, filters will contain only capacitors between each side of the line and chassis. The capacitors will be sufficiently low in value to allow less than 5 mA of current to flow to the chassis under the most adverse conditions of maximum power, frequency, and maximum voltage permitted by the individual test equipment specification. The design of the test equipment will be such that it will operate safely and in accordance with the applicable specifications with a ground on either side of the power source line. The primary line will be protected or fused except that the ground or neutral line will not be protected or fused.

15. All input power cables and interconnecting cables to other equipment—with the exception of radio frequency cables—will be provided with a grounding wire. The grounding wire will be connected through a terminal in the connector to the chassis or frame and will be used solely for the purpose of providing a ground potential. Power return wires are not to be used as grounding wires.

16. Assemblies will be bonded and grounded to provide for the discharge of static electricity.

17. The path to ground from the equipment will
a. Be continuous and permanent
b. Have ample carrying capacity to conduct safely any operating or fault currents that may be imposed upon it
c. Have impedance sufficiently low to limit the potential aboveground and to facilitate the operation of the overcurrent devices in the circuit. Inactive wires installed in long lines (conduit or cables) will be grounded to allow for stray or static electricity discharge.
d. Have sufficient mechanical strength to minimize the possibility of ground disconnection.

18. Ground connections to the chassis or frame will be mechanically secured by soldering to a spot-welded terminal lug, to a portion of the chassis or frame that has been formed into a soldering lug, or by use of a terminal on the ground wire that is then secured by a screw, nut, and lockwasher.

19. Devices will be provided to discharge high-voltage circuits and capacitors unless they discharge to 30 V within 2 s or less. Additional provisions are
a. These protective devices will actuate automatically when the case or rack is opened.
b. Shorting bars will be actuated either by mechanical release or by an electrical solenoid when the door or cover is open.

20. Grounding rods will be provided for all transmitting equipment where voltages are in excess of 70 V rms.

21. The system will be designed to provide protection against lightning strikes. Safeguards will be provided to minimize the effects of current flow, induced electrical fields, and other means of damage.

22. Shielding or armor on the cable will

a. Be grounded to the chassis or frame in the manner specified in Item 17

b. Be secured to prevent its contacting exposed current-carrying parts or grounding to the chassis or frame at any point other than the ground termination

c. Be terminated a sufficient distance from exposed conductors to prevent shorting or arcing between the conductor and the shielding.

23. The following protection will be provided to prevent shock injury:

Voltage V (rms or dc), V	Safeguards Required
$30 \leq V$	None
$30 < V \leq 70$	a. Protection required against accidental contact during normal operation of complete equipment and when changing fuses or electron tubes.
	b. Automatic discharge from capacitor circuits so they discharge to less than 30 V within 2 s.
$70 < V \leq 500$	a. All contacts, terminals, and like devices in this range will have barriers or guards. The barriers or guards will be marked with the approximate highest voltage (nearest round number) that may be encountered upon removal.
	b. If the provisions of the previous subpar. a are not satisfied, the doors, covers, or plates of a compartment of a major unit will be provided with an interlock that removes all potentials from exposed terminals in excess of 70 V rms when opened. The interlock may be of either a bypass or nonbypass type.
	c. Access to capacitor circuits or devices that do not discharge to 30 V or less within 2 s will be interlocked, as indicated in previous subpar. b, or provided with a suitable grounding rod and grounding connection.

d. When the operation or maintenance of equipment employing potentials in excess of 300 V peak could require that these voltages be measured, the equipment will be provided with test points so that all high voltages can be measured at relatively low potential level.

e. In no case will the potential exceed 500 V peak, relative to ground.

f. Full details will be given in the instruction book or maintenance manual of the method used to obtain the voltages at the test points in the equipment.

$V > 500$

a. The compartment doors, covers, or plates of a major unit operating above 500 V will be provided with interlocks having no bypass unless the assembly or device operating at a potential greater than 500 V or more is itself completely enclosed.

b. A completely enclosed assembly or device operating at a potential greater than 500 V, which can be opened when installed in the equipment, will be separately interlocked.

c. Access to a capacitor circuit or device that does not discharge to 30 V or less within 2 s will be interlocked, as indicated in previous subpar. b, with no bypass or provided with a suitable grounding rod and ground connection.

d. All contacts, terminals, and like devices operating in this range and their accesses will be clearly marked "DANGER HIGH VOLTAGE (MAXIMUM VOLTAGE APPLICABLE) VOLTS" with markings in accordance with ANSI Z35.1 (Ref. 89). Markings will have the normal life-expectancy of the equipment on which they are affixed and will be placed as close as possible to the point of danger. This requirement will be on a unit-terminated basis and is not intended to apply to individual tie points within a unit.

e. Encapsulated high-voltage assemblies with no other accesses need not be interlocked to prevent shock injury.

f. Cable connections with potentials in excess of 500 V rms or dc will be separately interlocked unless

    (1) Other provisions are made to insure that the supply power has been turned off prior to cable disconnect.

    (2) The small size of the connector precludes the use of an interlock.

In no case, however, should cable connectors be designed to expose conductors during disconnect, e.g., an extension cord has recessed female pins.

24. Unless otherwise specified, interlock switches will conform to one or more of the following:

    a. A two-piece type in which the electrical circuit is broken by the physical separation of the two parts

    b. A two-piece type in which the electrical circuit is broken by the physical separation of the two parts together with an associated electrically integral bypass device

    c. A one-piece switch assembly with an integral bypass device.

25. Any bypass switch or device will be such that returning the chassis to its operating position, or closing the door, cover, or plate, will automatically open the bypass switch and leave the interlock in position to function normally. Visual means will be provided to indicate when the interlock switch is bypassed.

26. Connections will be held to a minimum, and nonessential electrical termination points will be eliminated. Separable connectors will be used only where frequent disconnection is required or necessary for product manufacture.

27. Connectors used to provide separation of, or connection to, multiple electric circuits will be selected so that it will be impossible to insert the wrong plug in a receptacle or other mating unit.

28. Connectors will be so arranged and wired that no "hot" leads are terminated in pins or other exposed contacts that might be accidentally shorted or touched.

29. All unmated connectors will be covered with moistureproof and vaporproof caps or otherwise suitably protected. For example, connectors on enclosed cabinet-mounted equipment need not be provided with protective caps unless an environmental hazard exists. Protective caps specified by military specifications or military standards will be used. Where such protective caps are not available, disposable plastic or metallic caps designed for the purpose will be used.

30. Pin connectors will be deenergized when disconnected (exposed).

31. Pin locations in a connector will minimize the possibility of pin-to-pin short circuiting because of bent pins, moisture, cut wire ends, or other conductive debris.

32. Mechanical strain on a connector, termination, or other electrical junction will be avoided by use of supports.

33. Current overload protection for the equipment will be provided by fuses, circuit breakers, or other protective devices for primary circuits.

34. Devices such as fuses, circuit breakers, time delays, cutouts, or solid-state current interruption devices will be used to open individual leads of a circuit whenever a fault occurs.

35. Protective devices will be connected to the load side of the main power switch unless neutral power sensing is essential for proper protection of the equipment.

36. All protective devices employed will be in a readily accessible, safe location.

37. All fuses affording protection to the equipment will be placed in a convenient, serviceable location so that they are readily replaceable.

38. Where fuses are employed, at least one extra fuse of each type and rating used—but a quantity of not less than 10% of the total—will be supplied and incorporated in the same compartment·as the fuse in use. The ampere rating of all fuses used in the equipment will be indicated adjacent to the fuse holder in letters at least 1.19 mm (3/64 in.) high. In addition, "SPARE" will be marked adjacent to each spare fuse post. Fuse ratings will be compatible with both starting and operating currents.

39. Panel-mounted fuse posts will be designed to permit renewal of fuses without the use of tools.

40. Fuses on equipment main power circuits will be located on the load side of the main power switch.

41. Fusing will be arranged so that fuses in branch circuits will open before the fuses in the main circuit.

42. Connections to fuse holders having a test prod hole will be such that the metal structure that terminates the test prod hole is connected to the load side of the fuse.

43. Protection of individual parts from failures of associated parts should generally not be afforded; however, protection of networks, such as pulse-forming networks, from the failure of a single circuit will be provided by disconnecting this circuit from the network for critical cases.

44. When circuit breakers are used, the restoring or switching device will be readily accessible to the operator. Additional provisions are

    a. The circuit breaker will give a visual indication when the breaker is tripped.

    b. Holding the switching device closed on an overload will not prevent tripping of the breaker.

    c. Multipole circuit breakers will be used for the three-phase equipment and will disconnect all phases if an overload occurs in any one phase.

45. Wire cables and branches will be secured to the chassis or structure in which they are installed. Clearance will be provided to prevent chafing on sharp edges or movable parts.

46. Wires and cables will not be routed through access covers, doors, similar closures, or other locations where they might chafe, rub, kink, crimp, or be cut or crushed.

47. Where wires or cables pass through shields or other metallic partitions, the passage holes will be fitted with replaceable insulating grommets.

48. Shielding on wires and cables will be secured in a manner that will prevent the shielding from contacting or shorting exposed current-carrying parts. The shielding will terminate at a sufficient distance from the exposed conductors of the cable to prevent shorting or arcing between the cable conductor and the shielding. The ends of the shielding or braid will be secured against fraying.

49. Conductors intended to carry pulses or other waveforms, and which may undesirably couple such signals into other conductors, will not be bound into a cable.

50. Clearance will be provided between wires or cables, and heat emitters—such as electron tubes, resistors, dynamotors, and heat sinks—to prevent deterioration of wires or cables from heat generated under service conditions.

51. The bending radius of polyethylene cable will not be less than five times the cable diameter.

52. Circuits that require noninterruption of power for efficient servicing may be provided with front panel momentary contact switches to override interlocks and permit access to the manual override of the interlock. Additional provisions are

a. The override switch will be automatically disengaged when the protected-access door, cover, or panel is closed.

b. Power to the equipment will not be interrupted when the override switch is being activated or disengaged.

53. When a battle-short switch is required on the main operating console or assembly to short circuit all safety interlocks, it will also include

a. A readily visible light that will indicate to personnel the battle-short switch is ON

b. Indicator lights that will illuminate all interlocks when the battle-short switch is ON.

54. If use of a battle-short switch could cause overloading and damage to a system, an evaluation will be made to determine which items could be damaged and the interval of time until first damage could occur. A caution label indicating this time limit and the reason will be placed close to the battle-short switch.

55. If specified in the individual equipment specification, terminals will be provided in each separate cabinet or console for connecting an external battle-short switch or switches. Additional provisions are

a. Test provisions will be simple, foolproof, and fail-safe.

b. The terminals will not degrade the required performance of the item in which they are contained or cause it to be damaged.

56. Protection will be provided in test point circuitry to prevent equipment failure that could result from external grounding of test points.

57. Overload or decoupling protection will be provided to prevent damage to the test provisions by item signals or characteristics that may exceed specified tolerances.

58. Unless otherwise specified in the equipment specification, meters will have provisions for overload bypass or alternate protection to eliminate high-voltage potential or current at the terminals in the event of meter failure.

59. Insulating materials used in the construction of circuit breakers will neither burn nor give off noxious gases when subjected to the electrical arcing found in circuit breakers.

60. Insulating materials subject to arcing on instantaneous high-current tripping will be nontracking when subjected to the specific current limit.

61. Unless otherwise specified, dielectric withstanding voltages will be 1000 V plus twice the rating as a minimum value.

62. Unless otherwise specified, insulation resistance will be 100 megaohms or more.

63. Whenever pressurization of electronic equipment is required, the case in which the equipment is contained will have sufficient strength to withstand applicable pressure differences. Tests will be required to verify the adequacy of strength and integrity of the cases.

10-15 ACCELERATION

Acceleration occurs when any vehicle, body, fluid, or other material experiences a change in velocity. Since velocity is a vector term, the change can be one of speed only, one of direction only, or a change combining both speed and direction. The word "acceleration" is used when velocity increases; "deceleration" is used when it decreases. Acceleration may occur when propulsive power is applied or when an object is dropped or otherwise affected by gravity, impacted by another object or force, or subjected to a centrifugal motion (a continuous change in direction). Deceleration, or negative acceleration, will occur under any braking action, slowing due to friction, or by impacting another object or the ground.

Objects in motion contain kinetic energy, which must be considered in any design problem. Small objects with high velocities can cause great damage or injury, e.g., a speeding bullet-like projectile. Massive objects moving at relatively low velocity, e.g., a tank, can also cause great damage or injury if they strike something or someone. The damage will result not from the motion itself but from the acceleration, deceleration, or other transfer of energy when the object collides with some other object.

One problem resulting from acceleration is the sloshing of liquids in their containers, or over the tops, when the vehicle carrying the containers accelerates or decelerates linearly. For example, when the vehicle rounds a curve, centrifugal force will cause the liquid to slosh toward the outside of the curve.

Spring-actuated devices may not perform properly if their normal action lies in the direction of the acceleration (or deceleration) occurring while the device is operated. Mechanical relays in electrical circuits can fail to make required contact or make contact inadvertently if subjected to this type of acceleration environment. Springs mounting sensitive equipment must be equipped with dampers or snubbers to limit their movement when the equipment is subject to large accelerations, e.g., in a vehicle traveling fast over rough terrain.

Impacts are the most acute and most common manifestation of deceleration. Impacts can occur by design or by accident—especially those resulting from falls and collisions. Another occurrence of deceleration is in "water hammer". Water hammer occurs when a valve is closed quickly in a high-velocity flow system; this action causes a sudden stoppage of the incompressible fluid mass against the valve, generally accompanied by noise and vibration. This sudden stoppage can cause the valve to break due to the sudden conversion of the kinetic energy of the fluid mass into another energy form. The resultant pressure increase resulting from the change from kinetic energy to potential energy can also rupture lines and fittings.

Impacts, resulting in rapid deceleration, are the most frequent cause of accident and injury. A person can be seriously injured or even killed by striking his head after a fall from a standing position; an injury or fatality could result from the sudden deceleration in an auto accident. Data from falls and aviation accidents and tests relate the forces and shapes of objects striking the human body to injury modes. As far as these forces and resulting injuries are concerned, actually there is no difference whether an object strikes the body or the body strikes the object if the same decelerations are experienced. Studies and experiments have shown that the ability of the human body to withstand an impact depends on

1. Velocity at impact
2. Magnitude of the deceleration
3. Orientation of the body on impact
4. Part of the body impacted.

A detailed discussion of these factors is contained in Ref. 90. Such studies and tests have resulted in the development of the information shown on Figs. 10-40, 10-41, and 10-42 (Ref. 90). The G_i in these figures are defined as follows:

$+G_x$ = human tolerance for impact in a rearward-facing direction, g-units
$-G_x$ = human tolerance for impact in a forward-facing direction, g-units
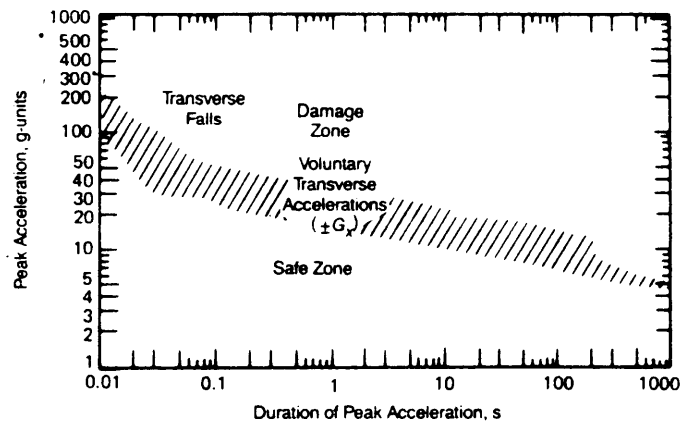
(A) Peak Transverse Acceleration Without Permanent Injury
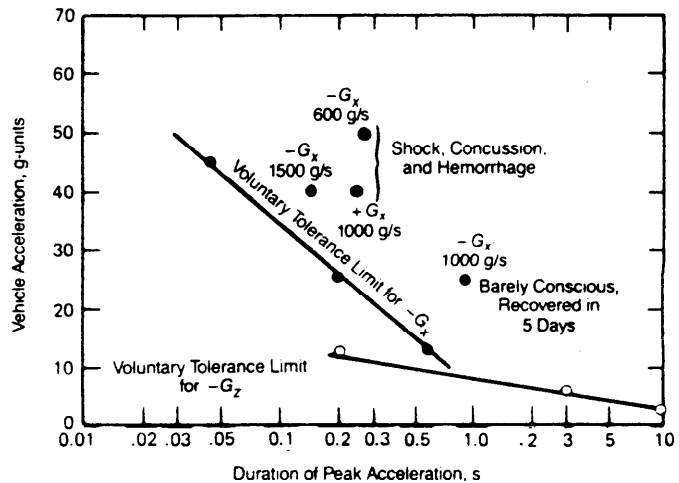
(B) Tolerance Limits for Vertical and Transverse Accelerations

Figure 10-40. Human Tolerance to Peak Accelerations (Ref. 90)

$+G_z$ = human tolerance for impact in a upward-facing direction, g-units
$-G_z$ = human tolerance for impact in a downward-facing direction, g-units.

A discussion of each of the figures follows.

Fig. 10-40(A) (Ref. 90) shows the peak transverse accelerations that humans survived without permanent injury. Peak accelerations lying below the hatched band are assumed to be noninjurious; the peak accelerations above the band have the potential for producing severe injury or death. Fig. 10-40(B) connects data points for the highest peak $-G_x$ and $-G_z$ accelerations voluntarily endured without injury by carefully restrained subjects. The four isolated points above the lines show accelerations that produced reversible but serious injury in the $\pm G_x$ acceleration.

Fig. 10-41 (Ref. 90) shows the impact sensitivity of the human body in terms of force per unit area for a $+G_z$
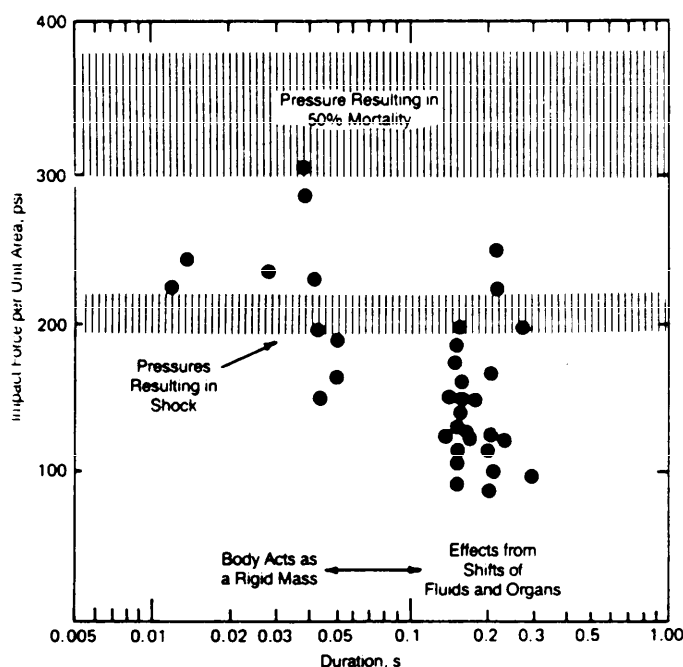
Figure 10-41. Impact Sensitivity of the Human Body (Ref. 90)
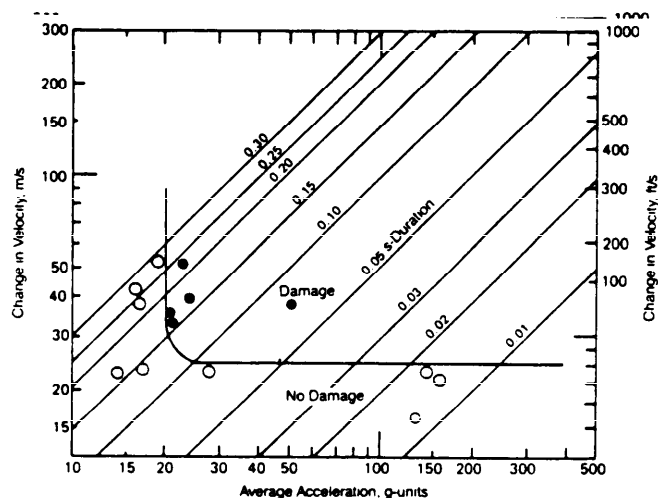
Figure 10-42. Regions of Damage and No Damage to Human Body Exposed to Various Levels and Duration of Acceleration (Ref. 90)

impact. The two shaded areas define approximate areas of effect in terms of impact pressure for any duration.

Fig. 10-42 (Ref. 90) shows the dividing line between mild injury (no damage) and severe injury (shock and retinal hemorrhage) for humans exposed to $+G_z$ impacts as a function of magnitude and duration of the applied force.

Vehicle collisions and the generation of lethal missiles resulting from collisions or impacts are the major sources of injury. Therefore, components that could break loose

and/or shatter under impact should be given special attention in the design of vehicles. Candidate materials for consideration are glass in windshields, windows, and rearview mirrors; highly stressed heat-treated metal parts for gun mounts or other load-carrying functions; and stressed plastic materials—all of which could shatter and produce hazardous missiles. Also the design should provide that the on-board items or equipment—tools, fire extinguishers, cargo, and ammunition—be secured in place because loose objects that could be displaced on impact may become deadly missiles. The shape of an object is also a factor in the amount of damage inflicted upon the human body in an impact. A blunt object of the same mass and velocity as a sharp object generally will inflict less damage than the sharp object because the impact forces are distributed over a larger area.

The kinetic energy of a body impacting on a hard surface is given by

$$KE = \frac{mv^2}{2}, \text{J}$$

$$= \frac{w(v')^2}{2g}, \text{ft·lb}$$

(10-10)

where

m = mass of object, kg
w = weight of object, lb
v = velocity, m/s
v' = velocity, ft/s
g = acceleration due to gravity = 32.2 ft/s².

By the use of Eq. 10-10, the velocity at which a body component will sustain injury can be computed. For example, a human head has a mass of approximately 5.4 kg (12 lb) and requires, on the average, 67.8 J (50 ft·lb) to fracture it. Thus the velocity at which the skull would fracture is

$$v = 2(KE)/m, \text{m/s}$$

(10-11)

$$= 2(67.8)/5.4 = 5.0 \text{ m/s} (16.4 \text{ ft/s}).$$

The 67.8 J (50 ft·lb) of energy could result by dropping an object with a mass of 2.27 kg (5 lb) through a distance of 3 m (10 ft).

The deceleration a of an object moving with a velocity v and brought to rest in a distance s can be computed by

$$a = v^2/(2s), \text{m/s}^2 (\text{ft/s}^2)$$

(10-12)

$$s = v^2/(2a), \text{m (ft)}$$

where

a = deceleration, m/s² (ft/s²)
v = velocity, m/s (ft/s)
s = stopping distance, m (ft).

If the deceleration a of Eq. 10-12 is divided by 9.81 m/s² (32.2 ft/s²), the result is expressed in g-units. As is evident from Eq. 10-12, a varies inversely as the stopping distance s—i.e., a decreases as s increases. By the use of Eq. 10-12, if the deceleration is given, the minimum distance s in which a body may be safely brought to rest at any velocity can be computed. This relationship is employed in the design of padding, bumpers, and collapsible engine and trunk compartments for vehicles. For design purposes it should be noted that the acceleration and distance relationships expressed in Eq. 10-12 assume a constant deceleration. Since padding, bumpers, etc., rarely provide this constant deceleration, additional padding may be required to insure a safety margin.

Table 10-45 (Ref. 90) provides information—other than the immediately apparent effects of bruises, broken bones, cuts, and skin penetrations—on internal injuries resulting from impacts. Because of these internal effects, persons who have been involved in collisions should be treated for shock.

10-15.1 TOLERANCES AND SAFE LIMITS

Table 10-46 (Ref. 15) indicates the biophysical factors that influence the degree of injury resulting from free falls. The same factors will apply to impacts due to collisions.

10-15.2 POTENTIAL HAZARD SOURCES

As previously indicated, most impact injuries in Army systems are due to collisions; however, impacts from falls may result from helicopter and aircraft operations. In some cases impact injuries have been sustained in aviation and ground vehicles that were not involved in accidents. These injuries occurred when the vehicles traveled over rough terrain or the aircraft encountered rough weather or made hard landings and unprotected occupants struck hard surfaces inside the vehicles.

A review of experimental experiences with impacts produced by short-track deceleration devices has shown that numerous physiological changes follow impacts in the transverse ($\pm G_x$) direction when the peak forces range from 15 to 25 G and onsets range from 400 to 1000 G/s. These are transient changes that occur in subjects who are entirely uninjured in the mechanical sense of bone fracture or detectable tearing of tissues and organs. The physiological changes are summarized in Table 10-45 (Ref. 90). The data in Table 10-46 (Ref. 15) provide information on biophysical factors related to the degree of injury suffered in free falls.

The source of falling objects that can cause injury or equipment damage may be beyond the control of the operators. The objects might be dropped by support or maintenance personnel, or the source might be the operators themselves, e.g., the operator could drop a heavy object on his foot. Self-inflicted injury is just as serious as that caused by another person.

Equipment in motion contains kinetic energy that must be converted into other forms of energy during deceleration. Equipment normally in motion while operating includes grinders, buffers, and other power tools; rotating devices such as turrets or wheels; and reciprocating machines such as saws, punches, and piston-driven equipment. These types of equipment can cause injury when the rotating components contact a person, which results in the body's absorbing some of the kinetic energy from the equipment. Rotating equipment such as grinders can be damaged when striking hard objects, which causes them to throw off fragments that can produce very serious injuries. (Grinding wheels can disintegrate—the result of centrifugal force—by being operated at speeds in excess of the safe operating speed.) These types of injuries can be avoided by providing equipment containment shields and covers and personnel-protective glasses and masks.

Impacts by fragments of pressure vessels that have ruptured violently can cause injury or damage. Equipment generating reciprocating motion can strike and injure unwary persons.

TABLE 10-46. LIST OF BIOPHYSICAL FACTORS THAT INFLUENCE DEGREE OF INJURY IN FREE FALLS (Ref. 15)

Physical Factors	Biological Factors
Duration of Impact	Age
Magnitude of Force	
(protective clothing-distance-velocity-air drag)	Sex
Impacted Material	Physical Condition
(deformation characteristics and contour)	Mental Condition
Direction of Force	
(orientation of body)	
Distribution of Force	Tissue Properties

10-15.3 DESIGN CONTROL TECHNIQUES

The best solution to prevent injuries due to acceleration, deceleration, or impact is to eliminate them by proper design. If impacts cannot be eliminated, the next best technique is to provide safeguards to avoid hard impacts.

If acceleration hazards are considered in the design process, then certain design features may be included to prevent injuries. Positive methods for attaching hardware, adequately strong materials to prevent unexpected failures, nonslip surfaces to prevent slips and falls, clearances adequate to avoid head impacts inside vehicles, and use of restraints are all design features to prevent injuries from falls and impacts. The equipment can have additional safeguards built in to minimize injuries caused by deceleration or impact. Restraints to secure occupants in a vehicle to minimize deceleration injury due to an impact or other sudden deceleration are indicated in Table 10-47 (Ref. 15). Refs. 91, 92, and 93 contain information useful to designers of helicopters to improve crashworthiness; this information can be used beneficially by designers of other Army vehicles. Ref. 92 provides additional information on aircraft seats, litters, personnel restraint systems, and hazards in the occupants' immediate environment.

The effects of acceleration or deceleration can be reduced by changing those factors listed in Table 10-46 so they will have the most beneficial effect (in lieu of detrimental effect) on the outcome of an impact or deceleration. For example, refer to Eq. 10-12; the deceleration can be reduced by increasing the stopping distance, and a small reduction in velocity will have a significant (power of 2) effect on the deceleration. The use of cushioning materials inside the vehicle will prevent injury by safeguarding the occupants from striking hard objects and will also lessen the deceleration by increasing the stopping distance. The elimination of sharp objects, points, and knobs will also reduce injury by impact. The use of materials and designs in the construction of the vehicle to absorb the energy in the event of an impact will minimize or avoid injury to the occupants of the vehicle by reducing the deceleration to the occupants. If somehow the duration of impact can be reduced, the effect is beneficial. This factor is not normally consistent with increasing the stopping distance, an event that requires more, not less, time for the occupant to come to rest.

Two other major beneficial effects may be created by changing the direction of force and distributing the force over a larger area of the body. These factors can only be used in a general manner since each situation is highly complex and most of the factors are interrelated. Thus each factor may be influenced by one or more other factors, and the conditions of the cause of the acceleration forces may also influence what factors are subject to change.

10-15.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

The following guidelines should be followed to protect against hazards due to impacts, accelerations, and decelerations:

1. Define reasonably foreseeable impact situations involving the equipment, operators, and potential non-operator exposure.

2. Determine in what manner (what events) parts (units, assemblies, and individual parts) can become part of the acceleration process, either in normal or abnormal operation.

3. Specify materials, shapes, and mountings of subsystems so the potential for injury or damage will be reduced when events defined in Item 2 occur.

4. Where there is a potential for operator impact with parts of the equipment, consider padding to reduce the hazard.

5. Use cages, restraining belts, or other operator restraint harness devices to isolate the operator's body and appendages from danger areas in any foreseeable type of situation.

10-16 MECHANICAL HAZARDS

Every piece of equipment may have the potential for presenting at least one type of mechanical hazard. For instance, mechanical hazards can be present in stationary materiel containing no moving parts but which may have sharp edges, corners, or points that may injure unwary personnel. Hazards of mechanical equipment in motion are especially common. Many of these types of hazards were covered in par. 10-15, "Acceleration". Mechanical hazards also include other situations such as articles of clothing or parts of the body getting caught in rotating or reciprocating machinery or getting parts of the body pinched, cut, or crushed between mechanical parts. Rotating gun turrets in Army equipment must also be considered in the safety analyses.

Probably the most common of all hazards are those involving mechanical equipment. The large number of reported accidents and injuries to people and equipment support this conclusion. The widespread use of mechanical equipment—particularly powered equipment—requires a thorough understanding of the hazards and the measures to prevent or to minimize the hazards.

If the weight of a piece of equipment or material is excessive, it can be a hazard if it is dropped or shifts position. The material may fall and injure someone, damage another piece of equipment, or damage itself. If equipment is unstable, it may tip or fall without warning and without human initiation.

TABLE 10-47. CONVENTIONAL AND ADDITIONAL RESTRAINT
FOR MAXIMUM BODY SUPPORT[1] (Ref. 15)

Direction of Acceleration	Vehicle Occupant	Body Position	Conventional Restraint	Additional Restraint for Maximum Body Support
Spineward	Operator	Seated facing forward	Lap strap Shoulder straps	Thigh straps
	Passenger or crew member	Seated facing forward	Lap strap	Shoulder straps Thigh straps Armrests and handholds Toe straps
Sternumward	Passenger or crew member	Seated facing backward	Lap strap	Backrest[2] Headrest[3] Chest strap[4] Leg and foot supports Armrests and handholds
Headward	Operator	Seated facing forward	Lap strap Shoulder straps	Thigh straps Chest strap[4] Headrest[3]
	Passenger or crew member	Seated facing forward	Lap strap	Shoulder straps Thigh straps Chest strap[4] Headrest[3] Armrests and handholds
		Seated facing backward	Lap strap	Chest strap[4] Headrest[3] Armrests and handholds
Footward	Operator	Seated facing forward	Lap strap Shoulder straps	None
	Passenger or crew member	Seated facing forward	Lap strap	Shoulder straps Handholds Toe straps
		Seated facing backward	Lap strap	Chest strap[4] Handholds Toe straps
		Supine	Lap strap	Webbed netting[5]

[1]Eiband, 1959
[2]Rigid with padded "wings"
[3]Full height, integral with backrest
[4]Armpit level
[5]Full support

Sharp edges, corners, and points are quite often the result of poor manufacturing processes, but sometimes they result from the desire to reduce manufacturing costs. They may also exist because the designer was unaware of the need to eliminate them. Even simple devices often have sharp edges, which can cause very deep wounds. In addition to the loss of blood and possible disablement when someone is cut or scratched by a sharp edge, there always is the possibility of infection that can lead to more serious complications. In some situations a sharp edge is necessary and cannot be eliminated. In these cases, protection is required to avoid injury. A cover or some other type of protective guard may be advisable, or the sharp edge may be located such that it is inaccessible and

will not cause injury. In most cases however, the sharp edge, corner, or point is not needed and can be removed during the manufacturing process.

Machinery in motion may be assemblies to stationary equipment—such as in power tools, rotating machinery, gears, conveyors, and many other types of mechanical devices—or they may be entire products such as vehicles. A prime hazard of machinery in motion is that parts of the body may be caught and crushed. Fingers are lost quite often in such situations. Rings and other jewelry are often caught by equipment, and this results in injuries. Other objects are often dropped into, or caught by, moving machinery, such that both the object and the equipment are damaged. Moving equipment can fail or be stopped when a tool or other hard object falls into it. The resultant jam can prevent mechanical controls from being operated, gears from turning, or it can cause chains to be thrown off sprockets and v-belts off pulleys.

When two moving surfaces come together or one surface moves against a fixed surface, they create a "nip" or "pinch point" where a finger, hand, or other part of the body could be caught and crushed, mangled, or severed. Occasionally, the two surfaces do not actually touch but come close enough to do considerable damage to anything caught between them. Examples of equipment with these pinch points or run-in points are

1. Meshing gears
2. Belts running over pulleys
3. Pressure rollers
4. Chains and sprockets
5. Cables on winch drums
6. Recoiling weapons, particularly in tank turrets.

Several examples of protective enclosures around these sources of potential hazards to personnel are shown in Fig. 10-43 (Ref. 41). The designer can adapt these techniques to other similar hazardous elements of Army equipment. A type of guard retaining the operator's arms and legs in a "cage" is used in an Army missile system to prevent injury to the gunner as the turret is rotated.

Many types of equipment used in the Army environment are large, bulky, and can be extremely heavy. A piece of equipment may be too heavy to be moved safely by one person, and an attempt to lift it can cause muscle injuries, especially of the back. The equipment may be so heavy that it cannot be moved safely without special equipment. It is also possible for the excessive weight to have an unusual center of gravity, which causes a shift in position as it is being moved, and which, in turn, may cause the item to fall or topple and injure someone or damage other equipment. Generally, the weight and the location of the center of gravity must be considered in the early design to minimize resultant problems. If unusual weight and center of gravity conditions are unavoidable,

the information should be placarded on the equipment, including the location of the center of gravity and designated lift points or attachments. If, as a last resort, it is determined that special handling equipment for transportation, installation, and maintenance is necessary, the design of the special equipment should be pursued along with the major equipment to avoid delays and unusual costs. Before deciding upon unique handling equipment, however, it is necessary to take cognizance of the real world of operation and maintenance, especially in the field. General-purpose handling equipment usually will be available, and personnel will be familiar with operation of it. Specialized equipment may not be available and, because of its infrequent use, personnel may not be familiar with the operation of it—a possibility which could result in an unsafe operation.

The size and shape of an object can also affect how safe it is. A piece of unstable equipment may topple or overturn and crush someone or damage other equipment. Small liquid containers are particularly vulnerable to overturning, and those that hold hot or corrosive fluids can cause injuries. Items that are tall in relation to the bases on which they rest tend to tip easily. Extensions that might move the center of gravity of the object to a point outside the base will cause the object to topple. Drawers of test benches extended during maintenance may cause this to happen, especially if the drawers are filled with heavy items and the bench is on an incline. Generally, such equipment can be secured to a floor or wall to prevent the tipping of it; otherwise the equipment should be made mechanically stable by designing the center of gravity low and in a position that will balance any movable parts such as drawers. Drawers and doors of benches or cabinets must also be provided with stops to prevent upsets.

10-16.1 TOLERANCE AND SAFE EXPOSURE LIMITS

To minimize injuries from sharp edges, specifications and standards require that exposed edges be rounded to a minimum radius of 1 mm (0.04 in.) (Ref. 91). Lifting standards are established by MIL-STD-1472 (Ref. 7) and summarized in Table 10-48 (Ref. 7). These weight limits are the maximum values that one man may lift, provided the item to be lifted is of convenient configuration, i.e., not more than 0.38 m (15 in.) long or 0.30 m (12 in.) high and equipped with suitable handles or grasp areas. The limits of Table 10-48 are not applicable for repetitive liftings or for tasks that require carrying the item for more than a few steps. Double the weight limits may be used as the maximum value for a two-man lift. Additional information relative to handles—dimensions and grasp surfaces—is contained in Refs. 7 and 13.
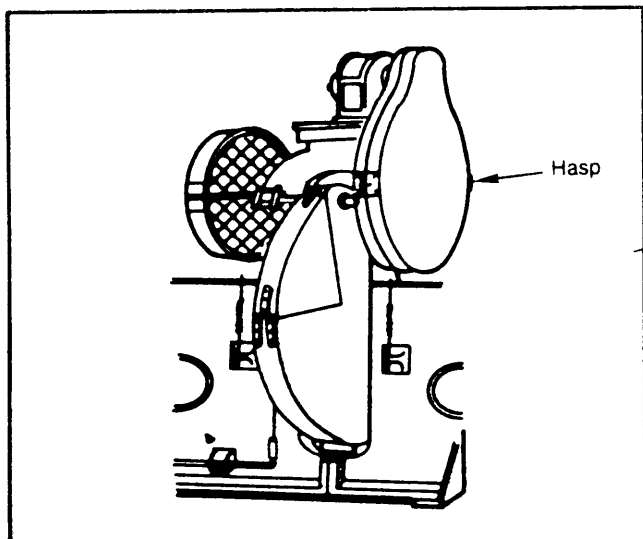
(A) Gears, Sprockets, Friction Drive

2-in. Minimum

2-in. Minimum

2 in.

6 in.

Shafting located under bench machines

Split sleeve anchored to machine frame

(B) Shafting Guards
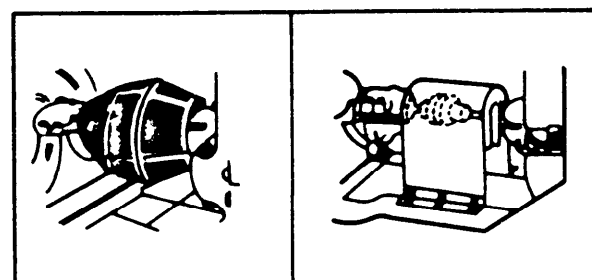
(C) Couplings, Collars, and Clutches

Sheet metal No. 24 or heavier

Iron pipe guard with wire cloth filler

Protection of rough edges

Wire mesh in 3/8-in. round rod frames

Expanded metal in 3/8-in. round rod frames

3/4 in. × 3/4 in. × 1/8 in. L

Perforated or sheet metal bolted directly to angle

Flat strip riveted or bolted angle to fasten filler

(D) Guard Construction

Hinge

Hasp
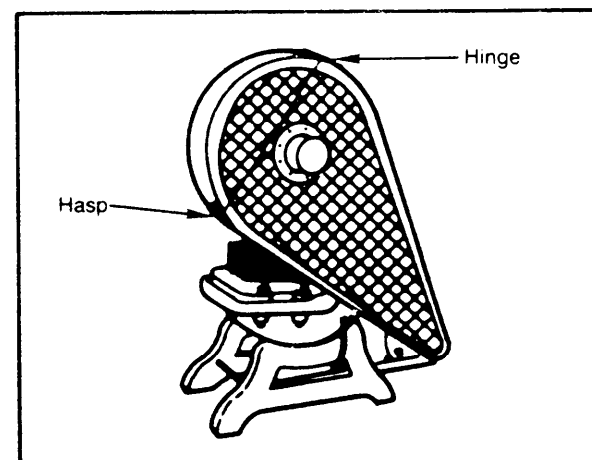
(E) Combination Belt and Pulley Guard

Figure 10-43. Protective Guards and Enclosures for Moving Parts (Ref. 41)
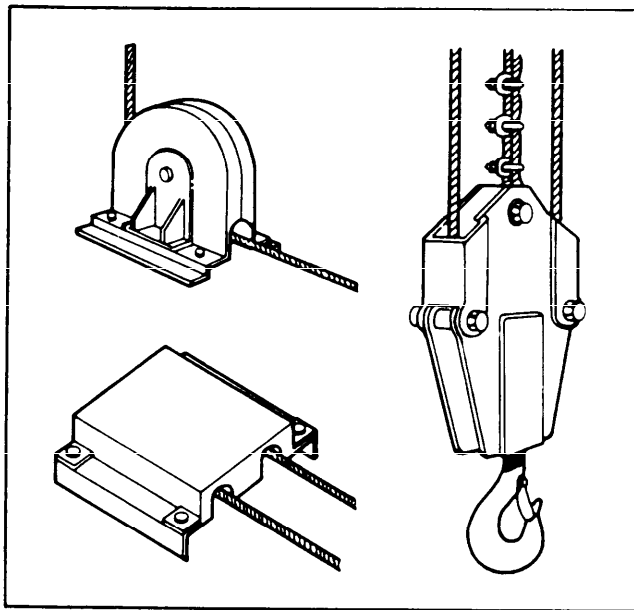
(F) Sheaves
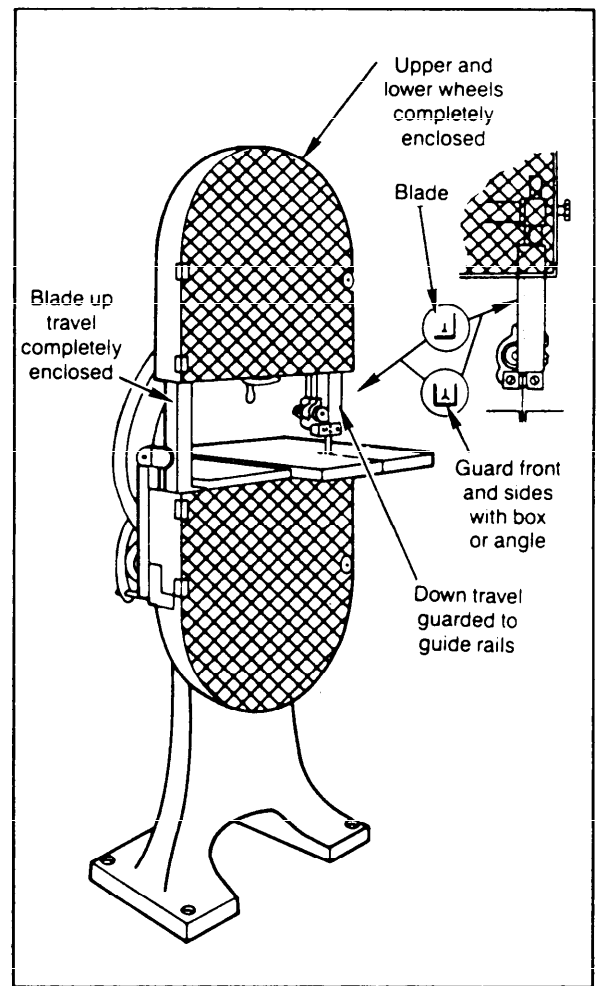
(G) Band Saws
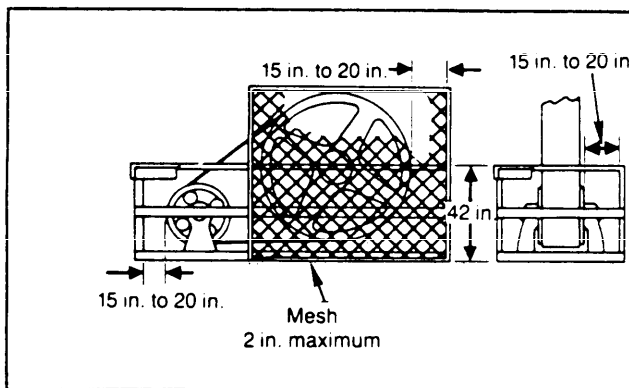
(H) Flywheels, Guard Rails
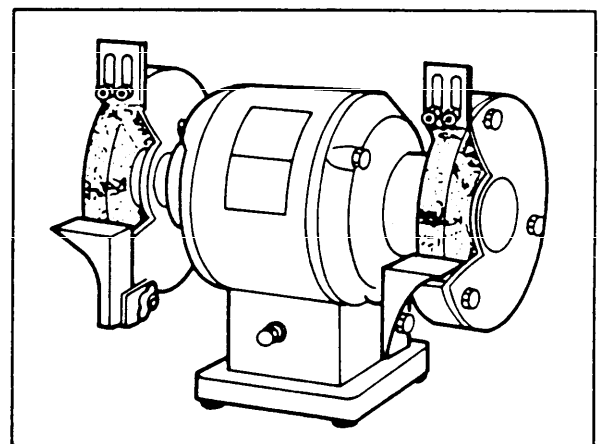
(I) Grinding Wheels

Figure 10-43   (cont'd)

TABLE 10-48. DESIGN WEIGHT LIMITS (Ref. 7)

Height of Lift From Ground	Maximum Weight of Item
1.5 m (5 ft)	16 kg (35 lb)
1.2 m (4 ft)	23 kg (50 lb)
0.9 m (3 ft)	29 kg (65 lb)
0.6 m (2 ft)	36 kg (80 lb)
0.3 m (1 ft)	38 kg (85 lb)

10-16.2 POTENTIAL HAZARD SOURCES

As previously indicated, all physical equipment can have mechanical hazards. The problems associated with sharp corners and edges, awkward weight, and traps to catch parts of the body have been identified. Another source of mechanical hazards not yet mentioned is failures of equipment that can cause injuries or damage. A very common example is the failure of a chain or rope used in hoisting that permits the load to drop. Not only will such failure generally cause damage to the load, but the falling load may crush and injure or kill personnel below. The whip effect associated with the snapping of a cable also can result in serious injury. Civil codes contain requirements for testing the design capacity of cranes. Other hoist devices should also be tested under safe test conditions before use. Designers should always consider the probable operating, maintenance, and support environment and provide safety factors in their designs of equipment where feasible.

10-16.3 DESIGN CONTROL TECHNIQUES

Mechanical hazards can often be controlled by using guards on the moving parts of machinery as illustrated in Fig. 10-43. If the moving parts are to be completely enclosed, other factors—such as heat buildup, vibration, and moisture entrapment—should also be considered. Guards or covers also will prevent inadvertent contact or introduction of foreign material into moving parts. In some instances substitution of materials may make the equipment safe without degrading its performance characteristics, e.g., using rubber fan blades instead of metal ones to reduce the possibility of injury. As an added protection, some moving machinery uses slip clutches. The clutch will slip if something is caught in the moving parts and cause a reduction in power, which can reduce the possibility of injury. Safety sensor devices are also a means to help prevent injury if a part of the body gets caught in the moving parts of a machine. The safety sensor device senses the entry of a foreign object into the machine, or the increased load, and stops the moving equipment.

The guards and safety devices must have certain characteristics to be effective and safe. Some of the characteristics are

1. They must be safe under all conditions. If they fail, cease to operate, or as in most cases, if they are opened, the machine must immediately and automatically stop.

2. They must prevent access to the danger zone while the equipment is operating.

3. They must impose no restrictions, discomforts, or difficulties to personnel.

4. They must automatically move into or be fixed in place.

5. They must be designed specifically for the equipment, the type of operations to be conducted, and the hazards that are present.

6. They must not require delicate adjustment for use or move out of adjustment easily.

7. They must be impossible for an operator to bypass or inactivate without simultaneously inactivating the equipment on which they are mounted. (Exceptions are for feeding, servicing, or testing units in a manner requiring continued operation.)

8. They should require minimum maintenance.

9. They should not constitute a hazard themselves.

The types of barriers and guards vary. Some are fixed and totally enclosed and allow no access or contact with the moving parts. Some are fixed with limited access, i.e., the guards or barriers have small openings that are generally not large enough for insertion of fingers or hands. Some are fixed with adjustable access; this feature enables the size of the opening to be changed to accommodate various materials. Others have movable barriers that allow quick access to the moving parts during maintenance and some operations.

Safety devices and sensors may be used to sense when there is an entry of some foreign material, or they may be interlocked to prevent unauthorized entry. There are a number of different safety devices to prevent injury during inadvertent entry of foreign materials. Optical sensors can be used to determine whether there is any object in the path of the moving parts. These sensors are usually a combination of a light source and a photocell target. They indicate when there is interference between the two. Ultrasonic sensors cover a wider area than a photoelectric sensor but are limited in range due to sound attenuation. Interlocks, by removing power if the cover or barrier is opened or removed, are also an effective means to prevent entry into moving equipment. See par. 9-5 for a complete discussion of interlocks.

The following precautionary measures are common to the operation and maintenance of all mechanical equipment:

1. All operators of mechanical equipment should be given training regarding hazards that may be present in the operation of the specific equipment. They should also

be aware of all incorporated safeguards and actions required in the event of an emergency.

2. Each operator should know the location and effect of STOP or EMERGENCY OFF buttons or switches on the mechanical equipment. The buttons or switches should be tested periodically to insure that they function correctly.

3. Equipment employing any type of guard or other safety device should be inspected at regular intervals to insure that the safety device is in place and is operable.

4. Each operator should be instructed against removing, inactivating, or attempting to circumvent any guard or safety device.

5. Repairs, adjustments, or maintenance that require removal of a guard or safety device should be accomplished only by trained and authorized personnel.

6. Operators of equipment in which clothing can be entangled should wear close-fitting clothes with button- or short-sleeved shirts. Jewelry, including rings and watches, should not be worn.

Specifications, standards, and other documents that contain design criteria for the control of mechanical hazards include

1. MIL-STD-1472, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities* (Ref. 7)

2. MIL-STD-454, Req. 1, *Standard General Requirements for Electronic Equipment* (Ref. 8)

3. OSHA 2206 (29 CFR 1910), *General Industry—OSHA Safety and Health Standards* (Ref. 29) (Although these standards apply to industrial work facilities, the information can be applied to Army systems.)

4. MIL-HDBK-759, *Human Factors Engineering Design for Army Materiel* (Ref. 13).

10-16.4 SAFETY CRITERIA FOR DESIGNERS TO FOLLOW

Criteria to be employed in the safe design of mechanical systems are

1. Safeguards will be provided to protect personnel from injury due to moving mechanical parts—such as gears, fans or belts, mounts, or other units in motion—when the equipment is in an assembled operating condition.

2. Guards will not prevent the inspection of mechanisms whose failure could cause a hazardous condition.

3. Either a positive lock, interlock, or disabling device will be provided to prevent operation of the hazardous unit when maintenance, adjustment, calibration, or other reason requires access to internal portions of the equipment or removal or bypassing of any safeguard. Additional provisions are

a. The positive lock may be a latch, pin, or similar block to prevent inadvertent action.

b. An interlock will be designed to inactivate the hazardous unit when the protective door, cover, panel, or guard, which provides access, is opened. An interlock with a bypass will be permitted only when a thorough analysis indicates that no serious injury can result. When an interlock with a bypass is used, it shall be

(1) Provided with a means of visually indicating that the interlock has been bypassed

(2) Of a type such that reassembly of the protective cover, panel, or other safeguard will automatically open the bypass and leave the interlock in position to function normally.

4. The mounting of rotating equipment will be sufficiently rigid to prevent damage due to motion with respect to its mounting.

5. Rotating equipment that is mechanically linked to operate with other devices will be mounted to prevent damage to the mating equipment, coupling, structure on which it is mounted, or any other associated device.

6. Any rotating equipment that can be damaged or can cause damage by impact during operation will be provided with at least two safeguards—e.g., hard stops, shock absorbers, hydraulic or pneumatic buffers, and flow limiters. A computer can be employed to sense impending damage and trigger the activation of these safeguards. Adequacy of the safeguards provided will be demonstrated by test.

7. Equipment will be so constructed that it will withstand, without damage, self-induced vibrations or shock, as well as vibration or shock encountered during shipment by air, ground, or sea, or other conditions to which it may be subjected.

8. Equipment will not vibrate to such an extent that it produces discomfort to personnel during its operation. Resonant frequencies will be avoided by proper design.

9. Shock and vibration isolation will be used only where it is impractical to design and construct the equipment to meet specified shock and vibration requirements or where shock or vibration could be injurious or damaging.

10. The envelope determined by the maximum movement of shock-mounted units will clear the surrounding structure and the maximum envelope of adjacent shock-mounted equipment by at least 6 mm (0.25 in.).

11. Shock-mounted units will not be mounted or installed in any manner other than that for which the shock mounts are designed. Cables and flexible hoses shall be of sufficient length to allow operation of shock mounts.

12. Cooling devices or any other attachments will not interfere with satisfactory shock mount operations.

13. Supporting members, brackets, racks, cable clamps, and mounting screws will be designed to carry units mounted thereon under the maximum acceleration, which can be expected in a vehicle under all operable

conditions, and to withstand incidental abuse.

14. Critical moving assemblies or elements of a system that can be damaged or jammed by dropped or loose articles, maintenance tools, debris, or shifting equipment will be protected by suitable screens, guards, covers, or other barriers.

15 When applicable, moving parts will be protected against water, fluid leakage, condensation onto and into the equipment, excessive heat, combustible vapors or fluids, physical damage by abrasion, personnel movements, loading or unloading, or similar hazards.

16. Large or heavy parts will be removable and replaceable without damage to surrounding components or danger to personnel.

17. When a chassis, subassembly, or other large unit is to be removable from its normal rack position or housing for maintenance or repair, it will be constructed for placement on any smooth surface without causing damage to any of its components.

18. Sharp corners, projections, and edges will be avoided on hardware items, cabinets, drawers, structures, and assemblies to which personnel have access.

19. Exposed edges will at least be broken but preferably rounded to a minimum radius of 1 mm (0.04 in.).

20. Exposed corners of large equipment that personnel encounter or use in day-to-day operations, such as desks or consoles, will be rounded to a minimum radius of 12.7 mm (0.5 in.).

21. Hinged covers on equipment enclosures will have devices to secure them in their open positions to prevent accidental closures, which could cause injury.

22. The weight limits in Table 10-48 will be adhered to. Items weighing more than the one-man life values of the table will be prominently labeled with weight indication and lift limitations, i.e., mechanical or two-man lift.

23. Where mechanical or power lift is required, hoist and lift points will be provided and clearly labeled.

24. Heavy items to be lifted mechanically will be provided with suitable lifting lugs or eyebolts and marked with the weight of the assembly to be lifted.

25. Safety-critical assemblies whose parts are fastened together will be secured against loss of joint integrity or separation when subjected to vibration or shock.

26. Except for those parts designed to be affixed with one fastener, parts will be secured so that failure of a single fastener will not free the part completely.

27. Friction between mating surfaces will not be employed as the sole means of preventing fixed parts from rotating or shifting.

28. For critically stressed applications, suitable torque values for screw thread assemblies will be established and torque measuring or controlling devices used for tightening the threaded parts.

29. For highly stressed applications, screws or bolts will have a minimum thread engagement of one and one-half times their nominal diameters in tapped parts other than nuts. In normal applications screws or bolts will have a minimum engagement length equal to their nominal diameter in tapped parts other than nuts. When the assembly is not frequently disassembled and where maximum strength is not required, less thread engagement may be used if special provisions are made to insure compliance with required conditions.

30. Where frequent disassembly (more than 15 times) is not expected, self-locking nuts will be used in lieu of lockwashers, except that self-locking nuts will be avoided on stud-mounted components unless the stud material is compatible with the strength or material of the nut used.

31. Castellated nuts with cotter pins may be used.

32. Where a bolt or screw is used without a nut, it will be either a self-locking type or secured by one of the following:

    a. Lockwasher under the bolt or screw head

    b. Self-locking thread insert

    c. Thread sealant

    d. Safety wire—0.8 mm (0.032 in.) minimum diameter—through the drilled head.

33. Retaining compounds, sealants, or nonmetallic retaining devices will not be used where

    a. Failure of the compound would endanger personnel or damage the equipment

    b. Service or processing conditions might deteriorate the material

    c. Disassembly is required and the strength of the fastener would be exceeded.

34. Brittle castings or parts made of ceramic or other brittle material will be cushioned to prevent breakage when being fastened. Washers or gaskets of suitable material and compressibility will be used between the otherwise facing surfaces of the brittle part and other brittle or metal parts to prevent breakage or damage during assembly or service. Lead washers will not be used.

35. Design will protect against damage to parts due to accidental use of bolts or screws that are too long.

36. Captive bolts and nuts will be used in situations where dropping such items might cause damage to equipment, create a difficult or hazardous removal problem, or generate any other unsafe condition, i.e., possibility of short circuit or jamming of controls or other movable devices.

37. Materials, fluids, and designs will be employed that will result in minimal friction, wear, and decomposition where contamination or corrosion could cause damage to, or failure of, safety-critical items in mechanical systems.

38. The system will be designed for maximum tolerance of contamination, i.e., use of greatest clearances and orifice sizes possible to minimize jamming or

plugging.

39. Where reversed or rotated mounting of a part cannot be tolerated, nonsymmetrical mounting arrangements (including keys or pins) will be used. Parts that will operate properly when mounted in any orientation are more desirable.

REFERENCES

1. MIL-STD-882B, *System Safety Program Requirements*, 30 March 1984.

2. AMCP 706-116, Engineering Design Handbook, *Environmental Series, Part Two, Natural Environmental Factors*, April 1975.

3. AMCP 706-117, Engineering Design Handbook, *Environmental Series, Part Three, Induced Environmental Factors*, January 1976.

4. J. E. Davidson, *et al.*, *Intriguing Accident Patterns Plotted Against a Background of Natural Environment Features*, Report SC-M-70-398, Sandia Laboratories, Albuquerque, NM, August 1970.

5. R. A. McFarland, *Human Factors in Air Transportation*, McGraw-Hill Book Company, New York, NY, 1953.

6. MIL-STD-1474B(MI), *Noise Limits for Army Materiel*, 18 June 1979.

7. MIL-STD-1472C, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities*, 2 May 1981.

8. MIL-STD-454J, *Standard General Requirements for Electronic Equipment*, March 1980.

9. TB MED 524, *Control of Hazards to Health From Laser Radiation*, June 1985.

10. MIL-STD-810D, *Environmental Test Methods and Engineering Guidelines*, 19 July 1983.

11. J. H. Thompson, T. E. Hill, C. V. Robinson, and J. M. Tierney, *Guidelines—Design to Minimize Contamination and to Facilitate Decontamination of Military Vehicles and Other Equipment: Interiors and Exteriors*, CRDC-SP-84023, US Army Armament, Munitions, and Chemical Command, Aberdeen Proving Ground, MD, August 1984.

12. W. Hammer, *Product Safety Management and Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

13. MIL-HDBK-759A(MI), *Human Factors Engineering Design for Army Materiel*, 30 June 1981.

14. ISO DIS 2631, *Guide to the Evaluation of Human Exposure to Whole-Body Vibration*.

15. H. E. Price and B. J. Tabachnick, *A Descriptive Model for Determining Optimal Human Performance in Systems, Volume III*, NASA CR-878, Ames Research Center, Moffett Field, CA, March 1968.

16. E. M. Roth, *Compendium of Human Responses to the Aerospace Environment*, NASA CR-1205(1), Lovelace Foundation for Medical Education and Research, Albuquerque, NM, November 1968.

17. S. L. Rezesman, *Report on Preobservations of Human Engineering Problems Under Desert Conditions*, TM 11, Human Engineering Laboratory, Aberdeen Proving Ground, MD, November 1954.

18. TB MED 507, *Occupational and Environmental Health, Prevention, Treatment, and Control of Heat Injury*, 25 July 1980.

19. Robert Berkow, M.D., Ed., *et al.*, *The Merck Manual of Diagnosis and Therapy*, Merck, Sharp, and Dohme Research Laboratories, Rahway, NJ, 1987.

20. MIL-STD-1522A, *Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems*, 28 May 1984.

21. MIL-H-5440G, *Hydraulic Systems, Aircraft, Types I and II, Design and Installation Requirements for*, 14 September 1979.

22. MIL-P-5518C, *Pneumatic Systems, Aircraft, Design, Installation, and Data Requirements for*, 9 July 1962.

23. *Code of Federal Regulations*, Cite 49 CFR 170.1, Transportation, Parts 100-199 (current revision).

24. C. L. Punte, "Particle Size Consideration of Airborne Contaminants", *A Symposium on Toxicity in the Closed Ecological System*, M. Honma and H. J. Crosby, Eds., Lockheed Missiles and Space Company, Palo Alto, CA, 1964.

25. *Threshold Limit Values for Chemical Substances and Physical Agents in the Workroom Environment With Intended Changes for 1981*, A Pamphlet Report, American Conference of Government Industrial Hygienists, Cincinnati, OH, 1981.

26. TB MED 268, *Medical Conditions Affecting Motor Vehicles and Equipment Operations*, February 1964.

27. *Cancer-Causing Chemicals, Cal/OSHA, Program*, State Division of Industrial Safety, Sacramento, CA, 1976.

28. TB MED 265, *Threshold Limit Values for Toxic Chemicals and Certain Electromagnetic Radiation*, April 1964.

29. *General Industry—OSHA Safety and Health Stan-*

dards, OSHA 2206 (29 CFR 1910), Occupational Safety and Health Administration, US Department of Labor, Washington, DC, June 1981.

30. TB MED 269, *Carbon Monoxide: Symptoms, Etiology, Treatment, and Prevention of Overexposure*, 31 May 1968.

31. Henning E. von Gierke, "On Noise and Vibration Exposure Criteria", Archives of Environmental Health **11**, 327-39 (September 1965).

32. E. B. Magid, *et al.*, *Physiological and Mechanical Response of the Human Body to Longitudinal Whole-Body Vibration as Determined by Subjective Response*, MRL-TDR-62-66, Aerospace Medical Research Laboratories, Wright-Patterson AFB, OH, June 1962.

33. Paul Webb, *Bioastronautics Data Book*, NASA-SP-3006, 1964.

34. H. M. Kinne, "Monitoring Machine Vibration", *Automation*, 50-6 (July 1969).

35. J. Campbell, "Measuring Noise", *Machine Design* (September 1967).

36. AR 40-5, *Health and Environment*, 1 July 1985.

37. TB MED 501, *Noise and Conservation of Hearing*, 7 March 1972.

38. T. R. Norris, *et al.*, *Development of Advanced Concepts for Noise Reduction in Tracked Vehicles*, Technical Memorandum 25-77, US Army Human Engineering Laboratory, Aberdeen Proving Ground, MD, August 1977.

39. "Design for Quiet", *Machine Design*, 174-224 (September 1967).

40. E. H. Berger, "Hearing Protector Performance: How They Work and What Goes Wrong in the Real World", *Sound and Vibration* (October 1980).

41. *Safety Engineering Standards*, Industrial Indemnity Company, San Francisco, CA, 1980.

42. *Nuclear Radiation Guide*, Report No. MRL-TDR-62-61, Aerospace Medical Division, Air Force Systems Command, Wright-Patterson AFB, OH, November 1962.

43. Robert C. Weast, Ed., *CRC Handbook of Chemistry and Physics* (current edition).

44. Clayton L. Thomas, M.D., M.P.H., Ed., *Taber's Cyclopedic Medical Dictionary*, F. A. Davis Company, Philadelphia, PA, 1981.

45. DA PAM 39-3, *The Effects of Nuclear Weapons*, April 1962.

46. W. Hammer, *Occupational Safety Management and Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1976.

47. Sol M. Michaelson, "Human Exposure to Nonionizing Radiant Energy—Potential Hazards and Safety

Standards", Proceedings of the IEEE **60**, 389-421 (May 1966).

48. TB MED 523, *Control of Hazards to Health From Microwave and Radio Frequency Radiation and Ultrasound*, July 1980.

49. David Sliney and Myron Wolbarsht, *Safety With Lasers and Other Optical Sources*, Plenum Press, New York, NY, July 1980.

50. *Aircraft Fire Safety*, Volume 2, AGARD-AR-132, NATO Advisory Group for Aerospace Research and Development, November 1979.

51. D. H. Sliney and B. C. Frasier, "Evaluation of Optical Radiation Hazards", *Applied Optics*, 1-24 (January 1973).

52. D. E. Busby, *Clinical Space Medicine: A Prospective Look at Medical Problems From Hazards of Space Operations*, NASA CR-856, Lovelace Foundation for Medical Education and Research, Albuquerque, NM, July 1967.

53. T.O. 31Z-10-4, *Electromagnetic Radiation Hazards*, 1 August 1966.

54. AR 385-11, *Ionizing Radiation Protection* (Licensing, Control, Transportation, Disposal, and Radiation Safety) (Includes requirements of 32 CFR 655.10), 1 May 1980.

55. AR 40-46, *Control of Health Hazards From Lasers and Other High-Intensity Optical Sources*, 6 February 1974.

56. ANSI Z136.1-1986, *Safe Use of Lasers*, American National Standards Institute, New York, NY, 23 May 1986.

57. R. A. Tell, "Broadcast Radiation: How Safe Is Safe?", *IEEE Spectrum*, 43-51 (August 1972).

58. DARCOM-R 385-29, *Laser Safety*, 9 August 1977.

59. F. G. Eichel, "Electrostatics", *Chemical Engineering*, 153-67 (13 March 1967).

60. M. G. Fontana and N. D. Greene, *Corrosion Engineering*, McGraw-Hill Book Company, New York, NY, 1967.

61. MIL-H-5606E, *Hydraulic Fluid Petroleum Base, Aircraft, Missiles, and Ordnance*, 2 March 1984.

62. MIL-H-83282C, *Hydraulic Fluid, Fire Resistant, Synthetic Hydrocarbon Base, Aircraft, Metric*, NATO Code Number H-537, 25 March 1986.

63. M. G. Zabetakis, *Flammability Characteristics of Combustible Gases and Vapors*, Bulletin 627, Bureau of Mines, US Department of the Interior, Washington, DC, 1965.

64. NFPA Manual 325M-1977, *Flammable Liquids, Gases, and Volatile Solids*, National Fire Protection Association, Inc., Quincy, MA, 1977.

65. C. J. Hilado and E. W. Clark, "Autoignition Tempera-

tures of Organic Chemicals", *Chemical Engineering*, 75-80 (September 1972).

66. R. Friedman and J. B. Levy, *Survey of Fundamental Knowledge of Mechanisms of Action of Flame-Extinguishing Agents*, WADC Technical Report 56-568, Wright Air Development Center, Wright-Patterson Air Force Base, OH, January 1957.

67. DARCOM-R 385-100, *Safety Manual*, 17 August 1981.

68. B. M. Dobratz, *LLNL Explosives Handbook — Properties of Chemical Explosives and Explosive Simulants*, UCRL-52997, Lawrence Livermore National Laboratory, Livermore, CA, 16 March 1981.

69. *Explosive Safety*, Executive Lecture Series, NASA N67-15981 through N67-15991, John F. Kennedy Space Center, Cape Kennedy, FL, June 1965.

70. MICOMP 385-4, *Safety, Ignition Systems for Army Rockets and Missiles*, US Army Missile Command, Huntsville, AL.

71. MIL-STD-1316C, *Fuze Design, Safety Criteria for*, 3 January 1984.

72. AMCP 706-205, Engineering Design Handbook, *Timing Systems and Components*, December 1975.

73. AMCP 706-210, Engineering Design Handbook, *Fuzes*, November 1969.

74. TB 700-2, *Explosive Hazard Classification Procedures*, August 1969.

75. "Static Electrification", *British Journal of Applied Physics*, Supplement No. 2, S1-S104 (1953).

76. H. F. Calcote, *et al.*, "Spark Ignition, Effects of Molecular Structure", Industrial and Engineering Chemistry **44**, 2659 (1952).

77. R. P. Himmel, "The Effects of Static Electricity on Thick Film Resistors", *Insulation/Circuits*, 41-4 (September 1972).

78. T. H. Pratt, *Streaming Currents*, HERC Newsletter No. 3A, Hercules, Inc., Cumberland, MD, October 1978.

79. R. L. Mondano and C. R. Buffler, *General Handbook of Electrical Grounding Concepts*, Custom Materials, Inc., Chelmsford, MA, November 1972.

80. *Lightning and Aircraft*, Lockheed Field Service Digest, Issue No. 48, Lockheed California Company, March 1964.

81. MIL-T-28800C, *Test Equipment for Use With Electrical and Electronic Equipment, General Specifications for*, 23 December 1981.

82. MIL-STD-1512, *Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods*, 6 January 1976.

83. MIL-STD-188/124A, *Grounding and Bonding for Common Long Haul/Tactical Communication Systems Including Ground-Based Electronic Facilities and Equipment*, 2 February 1984.

84. MIL-B-5087B, *Bonding, Electrical and Lightning Protection for Aerospace Systems*, 24 December 1984.

85. William S. Watkins, "GROUNDING: The Most Misunderstood of All Electrical Safety Requirements", *ASSE Journal*, 25-31 (January 1978).

86. NFPA 70-1981, *National Electric Code (NEC)*, National Fire Protection Association, Quincy, MA, 1980.

87. CAL/OSHA Pamphlet S-515, *Lockout/Blockout*, June 1981.

88. R. Beach, "Controlling Static Electricity With Electrostatic Neutralizers", *Product Engineering*, 177-81 (October 1953).

89. ANSI Z35.1-1972, *Specifications for Accident Prevention Tags*, American National Standards Institute, New York, NY, 1972.

90. James F. Parker, *et al.*, *Bioastronautics Data Book*, prepared for Office of Naval Research by Bio-Technology, Inc., Falls Church, VA, September 1972.

91. J. W. Turnbow, *et al.*, *Crash Survival Guide*, Technical Report 67-22, US Army Aviation Materiel Laboratories, July 1967.

92. S. P. Desjardins, *et al.*, *Aircraft Crash Survival Design Guide, Vol. IV—Aircraft Seats, Restraints, Litters, and Padding*, Simula Corporation, Tempe, AZ, June 1980.

93. D. H. Laananen, *et al.*, *Aircraft Crash Survival Design Guide, Vol. III—Aircraft Structural Crashworthiness*, Simula Corporation, Tempe, AZ, August 1980.

GLOSSARY

A

Abate. To eliminate or reduce permanently a safety or occupational health deficiency by coming into compliance with the applicable standard(s).

Acceleration. The rate of change of velocity. (When the change is negative, it is usually called "deceleration".)

Accessible Emission Limit (AEL). Maximum accessible emission level within a particular class.

Accident. Any unplanned event or series of events that results in death, injury, or illness to personnel or damage to or loss of equipment or property, i.e., mishap.

Allergic Rhinitis. Inflammation of the mucous membrane of the nose.

Alpha Particle. A positively charged nuclear particle identical with the nucleus of a helium atom.

Alternative System Design Concept. Additional systems to be considered along with the original design concept.

Alveolar Gas. Of, or relating to, or constituting a part of the air cells of the lungs.

Ambient. Surrounding on all sides, i.e., temperature, atmospheric pressure, illumination, etc.

Amplitude. The extent of a vibratory movement measured from the mean position to an extreme.

Analysis. An examination of a complex item, its elements, and their relations.

Anoxia. The absence of molecular oxygen in living tissue cells; often used to indicate reduction of the oxygen content of the blood below physiological levels.

Articulating. To form or fit into a systematic whole.

Asphyxiants. Materials that prevent an adequate oxygen supply to the body.

Asymptotic. A straight line associated with a curve such that as a point moves along an infinite branch of the curve, the distance from the point to the line approaches zero and the slope of the curve at the point approaches the slope of the line.

Autoignition Temperature. The temperature at which a material ignites spontaneously in air. (Also called spontaneous ignition temperature.)

Avionics. The development and production of electrical and electronic devices for use in aviation, missiles, and astronautics.

B

Backout and Recovery. The action(s) necessary in a contingency to restore normal safety conditions and to avoid a potential accident.

Beta Particle. A high-speed electron or positron.

Bistable. Capable of having two stable states, two dimensions, or two conditions.

Blast. The shock wave emitted from a point of detonation. Includes a shock front, a high-pressure area behind the shock front, and a rarefaction.

Blocking Element. A condition or device that prevents occurrence of another event, such as a fuze in the safe condition.

Boolean Logic. A combinatorial system that represents symbolical relationships (as those implied by the linguistic operators AND, OR, and NOT) between entities.

C

Carboxyhemoglobin. A product of reaction between hemoglobin and carbon monoxide. (Shown as COHb.)

Catastrophic Failure. A single failure that can result in death, severe injury, or loss of system.

Combustible. A material capable of burning under normal conditions. (A material that is flammable is easily ignited and highly combustible.)

Combustion. An exothermic reaction usually, but not necessarily, associated with oxidation of a fuel by atmospheric oxygen.

Combustion Products. Gases and solid particulates and residues evolved or remaining from a combustion process.

Compensating Provision. Actions that are available or

that can be taken by an operator to negate or mitigate the effect of a failure on a system.

Conduction. The transfer of heat by the motion of molecules from one portion to another portion of a substance without the movement of the substance itself. (In like manner, heat may be transferred by conduction from one substance to another when the two substances are in contact.)

Contaminants. Chemical, biological, or nuclear materials that have been developed for the specific purpose of killing or incapacitating people. (Other materials or agents developed for other military-related purposes, such as defoliation, also can have adverse effects on human and animal life; however, these other agents are not considered to be contaminants.)

Contingency. Abnormal situation that could deteriorate into an accident.

Contingency Analysis. A type of analysis conducted to determine procedures, equipment, and materials required to prevent a contingency from deteriorating into an accident.

Contractor. A private sector enterprise or the organizational element of DoD engaged to provide services or products within agreed limits specified by the managing activity.

Convection. The transfer of heat through a liquid or gas by movement of the molecules within the fluid. (Circulation of a fluid is a convection process caused by differences in the density of a fluid heated or cooled by whatever means—natural convection. Circulation can also be created by pumps, blowers, or agitators—forced convection.)

Corrective Action. A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency.

Cost-Effective. Economical in terms of tangible benefits produced by money spent.

Countermeasure. Any technique, device, or method designed to eliminate or reduce hazards, unsafe conditions, or unsafe acts.

Crashworthiness. The capability of a vehicle to protect its occupants against an accidental impact.

Critical Failure. A failure that may cause a mission abort, mission failure, personal injury, or equipment damage.

Critical Item. For safety, an item whose failure or operation could lead or contribute to an accident.

Criticality. A measure of the impact of a failure mode on

the mission objective. (Criticality combines the frequency of the occurrence and the level of severity of a failure mode.)

Criticality Analysis. A procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

Cryogenic. Of, or relating to, very low temperatures.

D

Damage. The partial or total loss of hardware caused by component failure; exposure of hardware to heat, fire, or other environments; human errors; or other inadvertent events or conditions.

Damage Effects. The result(s) or consequence(s) a damage mode has upon the operation, function, or status of a weapon system or any component thereof. (Damage effects are classified as primary damage effects and secondary damage effects.)

Damage Mode. The manner by which damage is observed. (Generally describes the way the damage occurs.)

Damper. A device designed to bring a mechanism to rest in a short time with minimum oscillation.

Damping. The extent of reduction of amplitude of oscillation in a mechanical system due to energy dissipation caused by friction, viscosity, etc.

Decibel (dB). A unit used to express sound pressure level. (The decibel level of a sound is related to the logarithm of the ratio of sound pressure to a reference pressure. The dB has meaning only when the reference quantity is known. The internationally accepted reference pressure in acoustics is 20 micropascals (μPa), which corresponds to 0 dB. This value is now used in most current acoustical literature. In the past, other units have been used (i.e., $20 \mu N/m^2$, 0.0002 μbar, 0.0002 dyne/cm^2), which are all physically equivalent to 20 micropascals.)

Decontamination. Any means of removing a contaminant from people or equipment or of neutralizing the effect of the contaminant.

Deflagration. Rapid burning with intense heat and brilliant light.

Degradation. A gradual impairment in ability to perform.

Deleterious. That which is considered to be hurtful or noxious.

Derating. Generally used in electronics: The use of components at stresses far less than those the manufacturer considers the components capable of sustaining.

Detection Mechanism. The means or methods by which a failure can be discovered by an operator under normal system operation or can be discovered by the maintenance crew by some diagnostic action.

Deterioration. Degradation in quality, mission accomplishment, and/or reliability due to age, usage, or environment.

Detonation. A reaction process with a flame front or shock wave that occurs at supersonic speed through the reacting medium.

Devolve. To pass by transmission or succession.

Diagrammatic Format. Graphic design that explains rather than represents; a drawing that shows arrangement and relations (as of parts).

Dielectric Constant. A measure of the ability of a material to resist conductance of an electric current.

Disequilibrium. Loss or lack of balance (equilibrium).

Dissociation. The process by which a chemical combination breaks up into simpler constituents.

E

Electromagnetic Radiation. The propagation of varying electric and magnetic fields through space at the velocity of light.

Electromagnetic Spectrum. The entire range of electromagnetic wavelengths or frequencies of electromagnetic radiation extending from gamma rays to the longest radio waves and including visible light.

Embedment. To place or fix firmly in surrounding matter.

Embolism. The sudden obstruction of a blood vessel by an embolus, i.e., an abnormal particle (as a gas or air bubble) circulating in the blood.

Emphysema. A condition of the lung marked by distension and frequently by impairment of heart action.

Encapsulate. To enclose in, or as if in, a capsule.

End Effect. The consequence(s) a failure mode has on the operation, function, or status of the highest indenture level.

Endothermic Reaction. A chemical reaction that requires the absorption of thermal energy.

Environments. The conditions, circumstances, influences, stresses and combinations thereof, surrounding and affecting systems or equipment during storage, handling,

transportation, testing, installation, and use in standby status and mission operation.

Equivalency TNT. The effects that can be generated by explosive or other explosion-producing material as measured in similar effects produced by a specific weight of trinitrotoluene (TNT).

Error. A human action not in conformance with a stipulated action, or one that violates normal, expected behavior so that it generates an accident.

Erythema. Abnormal redness of the skin (as in inflammation).

Euphoria. A feeling of well-being or elation.

Exothermic Reaction. A chemical reaction that results in the release of thermal energy.

Explosion. A rapid exothermic reaction characterized by a catastrophic buildup of pressure and resulting in a shock wave.

Explosion Limit. The highest or lowest concentration of a flammable gas or vapor in air that will explode when ignited.

Explosive. A substance capable of a sudden high-velocity reaction with the generation of high pressures.

Exposure Time. The period (in clock time or cycles) during which an item is exposed to failure measured from when it was last verified functioning to when it is verified again.

External Event. Those events over which the designer of the item has no authority.

Event. An occurrence that causes a change of state.

F

Fail-Safe Design. A design that interposes a safeguard to prevent a failure, materiel or human, from causing an accident.

Failure. Any deviation from the design-specified, measurable tolerance limits that cause either a loss of function or reduced capability.

Failure Analysis. The logical, systematic examination of an item or its diagrams to identify and analyze the probability, causes, and consequences of potential and real failures.

Failure Cause. The physical or chemical processes, design defects, quality defects, part misapplication, or other processes that are the basic reason for failure or that

initiate the physical process by which deterioration proceeds to failure.

Failure Effect. The consequence(s) a failure mode has on the operation, function, or status of an item. (Failure effects are classified as local effect, next higher level, and end effect.)

Failure Mechanism. The physical, chemical, electrical, thermal, or other process that results in failure.

Failure Minimization. Designed or programmed actions to reduce possibilities of failures to the lowest rates possible.

Failure Mode. The manner by which a failure is observed. (Generally describes the way the failure occurs and its impact on equipment operation.)

Failure Modes and Effects Analysis (FMEA). A procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity.

Failure Modes, Effects, and Criticality Analysis (FMECA). A method of reliability analysis that systematically reviews all components and materials in a system or product to determine causes of their failures, the downstream results of such failures, and how critical such failures might be as accident causes.

Failure Rate. The total number of failures within an item population divided by the total number of life units expended by that population during a particular measurement interval under stated conditions.

Fault. An undesired anomaly in the functional operation of an equipment or system.

Fault Hazard Analysis (FHA). A method of safety analysis that generally lists only those items in an FMECA that could contribute to an accident and omits other reliability considerations.

Fault Isolation. The process of determining the location of a fault to the extent necessary to effect repair.

Fault Tree. A graphic representation of the various parallel and series combinations of subsystem and component failures that can result in a specified system fault. (The fault tree, when fully developed, may be mathematically evaluated to establish the probability of the ultimate undesired event occurring as a function of the estimated probabilities of identifiable contributory events.)

Fault Tree Analysis (FTA). A graphic method of safety analysis by which possibilities of occurrence of specific adverse events are investigated. (After selection of the adverse event, all factors, conditions, events, and relationships that could contribute to that event are indicated. Then each of these contributing items in turn is studied for causes.)

Fire Classes. Classification of fires are according to the type of combustible involved:
Class A—Ordinary combustibles such as wood, cloths, paper, rubber, and certain plastics.
Class B—Flammable or combustible liquids, gases, greases, and similar materials.
Class C—Energized electrical equipment.
Class D—Combustible metals such as magnesium, titanium, zirconium, sodium, or potassium.

Fire Point. The lowest temperature at which a liquid gives off sufficient flammable vapor to produce sustained combustion after removal of the ignition source.

Firmware. A computer program that is stored in a fixed or "firm" way, usually in a read-only memory. (Changes can often be made only by exchanging the memory for an alternative unit.)

Flammability Limits. The maximum and minimum amounts of combustible gas in air, i.e., concentrations (by volume), that are capable of propagating a flame.

Flammability Range. The range between the lower and upper flammability limits.

Flash Point. The minimum temperature at which a liquid vaporizes sufficiently to form an ignitable mixture with air.

Fragmentation. An explosion during which material is splintered into fragments that are thrown in all directions.

Frequency. The number of repetitions or cycles of pressure variations of a sound per unit of time.

Function. The special purpose performed by an item.

Fungal Growth. Of, relating to, or having the characteristics of a growing organism called a fungus.

Furunculosis. A localized inflammatory swelling of the skin and underlying tissues (a boil).

G

Gamma Ray. A photon or radiation quantum emitted spontaneously by a radioactive substance.

Gates. In a fault tree analysis, the relationship between input events that could cause an output effect. An AND gate requires that *all* input events occur to generate an output event. With an OR gate, each and *any* of the input events could generate an output event.

H

Hardware. The mechanical, magnetic, electronic, and electrical devices from which a computer is fabricated; the assembly of material forming a computer.

Hazard. A condition that is prerequisite to an accident.

Hazard Level. A measure of the potential severity of a hazard based upon the worst case effects of personnel error, environment, design characteristics, procedural deficiencies, or subsystem or component failure or malfunction.

Hazard Probability. The likelihood, expressed in quantitative or qualitative terms, that a hazard will occur.

Hazard Severity. A qualitative assessment of the worst potential consequence, defined by the degree of injury, occupational illness, property damage, or equipment damage that could ultimately occur.

Hazardous. That which may pose an unreasonable risk to health and safety or property.

Hazardous Event. An occurrence that creates a hazard.

Health Hazard. An existing or likely condition inherent to the operation, maintenance, storage, or disposal of materiel or a facility that can cause death, injury, acute or chronic illness, or disability.

Health Hazard Assessment. The application of biomedical and psychological knowledge and principles to identify, evaluate, and control the risk to the health and effectiveness of personnel who test, use, or service Army systems.

Hidden Failure. Failure that is undetectable during operation by the operator or crew.

High Explosive. A material that normally detonates when subjected to heat or shock that initiates a violent disassociation of its molecules.

Human Error. Mistakes that are representative of the sympathies and frailties of man's nature.

Human Factors Engineering. A comprehensive technical effort to integrate into Army doctrine, materiel development, and materiel acquisition (to insure operational effectiveness) all relevant information on human characteristics, skill capabilities, performance, anthropometric data, biomedical factors, safety factors, training, and manning implications.

Hydrostatic Head. Pressure exerted by a volume of liquid at rest.

Hypergolic. The property of two substances that causes the substances to ignite spontaneously when mixed together.

Hyperpyrexia. Exceptionally high fever.

Hypoxia. A deficiency of oxygen reaching the tissues of the body.

I

Ignition Energy. The quantity of heat or electrical energy that must be absorbed by a substance to cause it to ignite and burn.

Ignition Source. Any agent that could initiate a fire or explosion.

Ignition Temperature. The minimum temperature to which a solid, liquid, or gaseous substance must be heated to initiate or cause self-sustained combustion independent of the heating element. (In solids, the ignition temperature may vary with particle size.)

Impact. A sudden deceleration of an object or body by hitting another object or body on a highly resistant surface.

Impulse Noise. Noise (also referred to as impulsive or impact noise or as blast overpressure), such as that produced by weapons fire, punch presses and drop hammers, consists of a short burst of acoustical energy. (Impulse noise is characterized by a rapid rise time of not more than 35 ms to a peak pressure. The total duration of a single impulse is not more than 500 ms. When the interval between peaks is 0.5 s or less, it is best to consider the noise source as "steady noise".)

Indemnification. To secure against hurt, loss, or damage.

Indenture Levels. The item level that identifies or describes the relative complexity of assembly or function. (The levels progress from the more complex (system) to the simpler (part) divisions.)

Infrared Radiation. Thermal radiation of wavelengths longer than those of visible light.

Inherent. Involved in the constitution or essential characteristics of something.

Inhibition. Reduction of a fire or flame by the introduction of a chemical or a cold surface that interferes with flame reactions.

Initial Indenture Level. The level of the total, overall item that is the subject of the failure modes, effects, and criticality analysis.

In-Process Review (IPR). A review of a project or program at critical points to evaluate the status and to make recommendations to the decision-making authority. (Formal IPRs are conducted by the materiel developer.)

Interfaces. The systems, external to the system being analyzed, that provide a common boundary or service and are necessary for the system to perform its mission in an undegraded mode, for example, systems that supply power, cooling, heating, air services, or input signals.

Interlock. A protective device to prevent human access to a hazardous area or to prevent or interrupt equipment operation unless other required conditions are satisfied.

Ionization. The formation of electrically charged particles; can be produced by high-energy radiation, such as light or ultraviolet rays, or by collision of particles in thermal agitation.

Ionizing Radiation. Electromagnetic radiation having a sufficiently large photon energy to ionize atomic or molecular systems directly with a single quantum event.

Irritant. Any substance that has the capability to injure, stimulate cells, or generate other adverse effects at the contact site.

Isolate. To separate from another substance to obtain purity or to set in a free state, i.e., to set apart from others.

Iteratively. Relating to, or being, a computational procedure in which replication of a cycle of operations produces results that approximate the desired result more and more closely.

K

Kindling Temperature. The lowest temperature at which a solid substance will ignite.

Kinetic. Of, or relating to, the motion of material bodies and the forces and energy associated therewith.

L

Laser. A source of intense, coherent, and directional optical radiation. Also an acronym for *light amplification by stimulated emission of radiation*. (A laser usually is composed of an energy source, a resonant cavity, and an active lasing medium.)

Latent Failure. A failure that is not inherently revealed at the time it occurs.

Lethalities. Of, relating to, or causing death.

Liability. Something that works as a disadvantage.

Life Cycle. The series of stages in form and functional activity through which a product, individual, group, or culture passes through its lifetime, i.e., a series of stages from concept to disposal of a product.

Local Effect. The consequence(s) a failure mode has on the operation, function, or status of the specific item being analyzed.

Lockin. A protective device that restricts personnel inside specific limits to prevent contact with a hazard outside those limits or that maintains the hazard inside those limits so that it cannot affect anything outside.

Lockout. A protective device that restricts personnel outside specific limits to prevent contact with a hazard inside those limits or that maintains the hazard outside those limits so it cannot affect anything inside.

Low Explosive. An explosive that normally deflagrates to produce a large amount of heat and gas.

M

Malfunction. To fail to operate in the normal or usual manner.

Marginal Failure. A failure that can degrade performance or result in degraded operation. (Special operating techniques or alternative modes of operation involved by the loss can be tolerated throughout a mission but should be corrected upon its completion.)

Maximum Permissible Exposure (MPE). The level of laser radiation to which a person may be exposed without hazardous effect or adverse biological changes in the eyes or skin.

Mediastinal. An irregular median septum or partition of the thoracic cavity.

Metabolism. The sum of the processes by which a particular substance is handled in the living body.

Microwave Radiation. A comparatively short electromagnetic wave that produces heat when penetrating matter.

Minimal Cut Sets. A smallest set of primary events, inhibit conditions, or undeveloped fault events, all of which must occur for the top event of a fault tree to occur.

Minor Failure. A failure not serious enough to be classified catastrophic, critical, or marginal, but which requires corrective maintenance.

Minor Loss Acceptance. A feature designed into a product or system where a failure will result, because of

an adverse event, that will generate a small, acceptable amount of damage so that a far more serious and greater amount of damage will not occur.

Mishap. An unplanned event or series of events that result in death, injury, occupational illness, or damage to, or loss of, equipment or property.

Mock-Up. A full-sized structural model built accurately to scale chiefly for study, testing, or display.

Mucosa. The body's mucous membrane.

N

Near Miss. An occurrence in which accidental injury or damage was narrowly avoided by chance and not by design.

Necrosis. Localized death of living tissue.

Neutron. An uncharged elementary particle that has a mass nearly equal to that of the proton and is present in all known atomic nuclei except the hydrogen nucleus.

Noise. In the nontechnical sense, any unwanted sound. (Noise may be steady, either a pure tone or a complex of tones, or it may consist of one or more impulses. The term is usually applied to sounds having a complex character with numerous separate frequency components extending over a wide range of frequencies and not generated to convey meaning or information.)

Nuclear Regulatory Commission. An independent agency of the Federal Government established 11 October 1974 to regulate, license, and supervise the security and safety of peaceful uses of nuclear power.

O

Offeror. The organization or individual who presents a proposal to do some specified act for remuneration.

Operating and Support Hazard Analysis. An analysis performed to identify and control hazards and to determine safety requirements for personnel, procedures, and equipment used in production, installations, maintenance, testing, modification, transportation, storage, operation, emergency escape, egress, rescue, training, and disposal during all phases of intended use as specified in the system requirements.

Operational Suitability. The degree to which a system can be placed satisfactorily in field use with consideration being given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistic supportability, and training requirements.

Operator. One who operates a machine or device.

Oscillate. To move or travel back and forth between two points; to vibrate.

Oxidizer. A substance that liberates oxygen or other substance that combines with a fuel in a combustion process.

Ozone. A triatomic form of oxygen that is a bluish, irritating gas of pungent odor.

P

Peak Pressure. The maximum force exerted against a unit area by a blast wave.

Pneumothorax. A state in which air or other gas is present in the pleural cavity. (Also a therapeutic measure to collapse the lung.)

Potentiate. To make more effective.

Power Density. The average intensity of electromagnetic radiation present at a given point. (The average power per unit of area, usually expressed as milliwatts per square centimeter (mW/cm^2).)

Preliminary Design Review (PDR). An examination and review of conceptual design drawings and logistics.

Primary Events. The normal terminus of a path of fault events within a fault tree.

Primary High Explosive. An explosive that is extremely sensitive to heat and is normally used to initiate a secondary high explosive.

Procedure Analysis. A method of reviewing proposed operations to determine that programmed steps or that failure to follow those steps will not generate accidents.

Proof Testing. Tests designed to meet the requirements of the several physical laws that prove the safety, reliability, and maintainability of a product.

Propellant. A low explosive that burns very rapidly (deflagrates) to produce a large volume of gas that creates enough pressure to propel a projectile or rocket.

Pulmonary Edema. Fluid in the air sacs and interstitial tissue of the lungs.

Pyrophoric. Igniting simultaneously.

Q

Qualitative. The term used to describe those inductive analytical approaches that are oriented toward relative, nonmeasurable, and subjective values.

Quantitative. The term used to describe those inductive or deductive analytical approaches that are oriented toward the use of numbers or symbols used to express a measurable quantity.

R

RAD. The absorbed dose of any ionizing radiation that is accompanied by the liberation of 10^{-5} J of energy per gram of absorbing material.

Radiation. The transfer of heat in the form of electromagnetic waves between two bodies, substances, or surfaces that are not in contact.

Random Failure. Failure whose occurrence is predictable only in a probabalistic or statistical sense. (This applies to all distributions.)

Redundancy. The existence of more than one means to accomplish a given function. (Each means of accomplishing the function need not necessarily be identical.)

Redundant System. A system composed of two or more components below major item level that are capable of performing the same mission or function independently of each other.

Reliability. The probability that an item will perform its intended function for a specified interval under stated conditions.

REM (roentgen equivalent man). The dosage of an ionizing radiation that will cause the same biological effect as one roentgen or X-ray or gamma dosage.

Replacement. The action or process of replacing some element of a chemical reaction.

Risk. An expression of possible loss in terms of hazard severity and hazard probability.

Roentgen. The international unit of x-radiation or gamma radiation equal to the amount of radiation that produces, in one cubic centimeter of dry air at $0°$ C and standard atmospheric pressure (760 mm Hg), ionization of either sign equal to one electrostatic unit of charge.

S

Safety. Accident-free conditions.

Safety Analysis. A systematic examination started early in the acquisition process (often during the concept exploration/definition phase) to determine the ways a system (or parts of it) will function in each operating mode, to identify potential hazards, to predict the potential of these hazards for injury to personnel and/or damage to equipment, and to determine ways to eliminate the hazard.

Safety Assessment Report (formerly Safety Statement). A formal summary of the safety data collected by the contractor or materiel developer during the design and development of the system. (In it the contractor or materiel developer states the hazard potential of the item and recommends procedures or corrective actions to reduce these hazards and to avoid personnel loss or injury or equipment damage during development testing.)

Safety Factor. Ratio of ultimate strength of a material to the allowable stress.

Secondary Damage Effects. The result(s) or consequence(s) indirectly caused by the interaction of a damage mode with a system, subsystem, or component thereof.

Self-Extinguishing. Incapable of sustained combustion in air after removal of external heat or flame.

Sensitivity. The characteristic of an explosive that expresses its susceptability to initiation by externally applied energy, or conversely, the ability of the explosive to withstand the effect of some kind of outside stimulus.

Sensitivity, Explosive. A measure of the mechanics involved and rapidity with which an explosive can be detonated.

Sequence Interlocks. An interlock or series of interlocks that insures that it is mechanically or electrically impossible to activate equipment in an improper sequence.

Severity. The consequences of a failure mode. (Severity considers the worst potential consequence of a failure, which is determined by the degree of injury, property damage, or system damage that could ultimately occur.)

Single-Point Failure. The failure of an item that would result in failure of the system and is not compensated for by redundancy or an alternative operational procedure.

Sneak Circuit. An unexpected path or logic flow within a system that, under certain conditions, can initiate an undesired function or inhibit a desired function. (Sneak circuits are *not* the result of hardware failure but are latent conditions that are inadvertently designed into the system and cause it to malfunction under certain conditions.)

Sneak Circuit Analysis (SCA). A procedure conducted to identify latent paths that cause occurrence of unwanted functions or inhibit desired functions assuming all components are functioning properly.

Sneak Indication. An ambiguous or false display of

system operating conditions that may result in an operator's taking an undesired action.

Software. The totality of programs and routines used to extend the capabilities of computers, such as compilers, assemblers, narrators, routines, and subroutines.

Software Safety Analysis. A study of a software program to insure that the program, used in its intended operational environment, cannot cause or contribute to a hazard to personnel or equipment.

Software Sneak Analysis (SSA). A computer-aided analysis that locates software errors that may cause an anomalous system function to occur. (An SSA is performed by using an adaptation of the techniques used in the sneak circuit analysis (SCA), which is a proven hardware safety and reliability technology.)

Sound Spectrum. A pattern of the distribution of energy or sound pressure in different bands along the scale of audible frequencies. (The spectrum can be determined by measuring the sound pressure in each of 10 bands one octave in width, covering the audible frequencies. The center frequencies of these bands are 31.5, 63, 125, 250, 500, 1000, 2000, 4000, 8000, and 16,000 Hz. These 10 bands are called the preferred series of octave bands, and the measurement is called an octave band analysis. One-third octave or narrow band analyses may be required for engineering control measures.)

Sovereign Immunity. The exemption of an autonomous power from certain regulations and laws of a host entity, i.e., diplomatic immunity of nations.

Spontaneous Ignition Temperature. The lowest temperature at which a flammable material can be ignited in a specified atmosphere and at a specified pressure without the use of a flame, spark discharge, or any other energy source. (Also called autoignition temperature.)

Steady Noise. A periodic or random variation in atmospheric pressure at audible frequencies. (It may be continuous, intermittent or fluctuating, with the sound level varying over a wide range. For example, high-intensity steady noise is commonly found in the interiors of tanks, personnel carriers, and truck cabs; near field electrical generator sets; in machine shops, carpenter shops, and engine repair and testing shops; in any area where air-driven tools are used; near or inside aircraft in operation on the ground and in flight; and near aircraft engines operated on stands.)

Storage Life. The length of time an item can be stored under specified conditions and still meet specified requirements.

Subsystem. An element of a system that, in itself, may constitute a system.

Synergism. The combined action or effect of two or more agents that is greater than the sum of their individual actions.

System. A composite, at any level of complexity, consisting of operational and support equipment, facilities, and software used as an entity and capable of performing and supporting an operational role.

System Analysis. A detailed examination of a system and its component parts.

System Safety. The optimum degree of safety and health features within the bounds of operational effectiveness, time, and cost, attained by using system safety engineering and management principles to identify hazards and reduce risks throughout the life cycle of a system.

System Safety Engineer. An engineer qualified by training and/or experience to perform system safety engineering tasks.

System Safety Engineering. An element of system engineering requiring specialized professional knowledge and skills in the application of scientific and engineering principles, criteria, and techniques for the timely identification and elimination or control of hazards.

System Safety Group/Working Group. A formally chartered group of persons, representing organizations associated with the system acquisition process, organized to assist the managing activity's program manager in achieving the system safety objectives.

System Safety Management. That part of system management that insures the planning, implementing, and completing of tasks and activities to meet system safety requirements consistent with overall program requirements.

System Safety Program. The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of the system life cycle.

System Safety Program Plan (SSPP). A written plan outlining the steps needed to combine the tasks and activities of system safety engineering and system safety management with other disciplines and functions to achieve system safety for a specific system.

Systematic Approach. An approach that will identify the maximum number of hazards in the system, identify their causes, predict their effects as accurately as possible, and recommend the most effective ways to eliminate or control the hazards.

T

Tabular Format. An expression of ideas, comparisons, trends, and values in graphic tables.

Threshold Limit Value (TL V). The airborne concentration of a substance (stipulated by the American Conference of Governmental Industrial Hygienists) to which all workers may be exposed for a working lifetime (8 h/day, 5 days/wk) without adverse effect.

Toxicity. The harmful effect of a chemical or physical agent on the physiological functions of a biological system.

Tradeoff Studies. A determination of what can be exchanged and the value of that exchange, i.e., giving up one thing in return for another.

Triboelectric Surface. A surface that will generate a charge of electricity when rubbed with certain materials, e.g., rubbing glass with silk.

U

Ultraviolet Radiation. Radiation beyond the visible spectrum and having a wavelength shorter than visible light and longer than that of an X ray.

Undetectable Failure. A postulated failure mode in the failure mode and effects analysis for which there is no failure detection method by which the operator is made aware of the failure.

Upper Limit of Flammability. The highest percent concentration by volume of a flammable vapor or gas in air that will burn.

V

Validation. To support or corroborate on a sound or authoritative basis, i.e., convincing and authoritative proof of validity.

Vasomotor. Of, relating to, or being nerves or centers controlling the size of blood vessels.

Verification. The development of data used to evaluate the safety and health features of a system to determine its acceptability. (This is done primarily during development test and evaluation and supplemented during user or operational test evaluation.)

W

Waived. To relinquish or abandon intentionally a known right, claim, regulation, or privilege.

X

X Rays. Extremely short wavelength radiations produced by bombarding a metallic target with fast electrons or by transition of atoms to lower energy states. (In addition to ionizing gases, X rays can produce secondary radiation by impinging on material bodies.)

INDEX

INDEX (cont'd)

INDEX (cont'd)

INDEX (cont'd)

INDEX (cont'd)

Custodian:
  Army - MI

Preparing activity:
  Army - MI

Review activities:
  Army - AL, AT, AV, CR, ER, ET, ME, TE

(Project SAFT-A020)

INSTRUCTIONS: In a continuing effort to make our standardization documents better. the DoD provides this form for use in submitting comments and suggestions for improvements. All users of military standardization documents are invited to provide suggestions. This form may be detached, folded along the lines indicated, taped along the loose edge (DO NOT STAPLE), and mailed. In block 5, be as specific as possible about particular problem areas such as wording which required interpretation, was too rigid, restrictive, loose, ambiguous, or was incompatible, and give proposed wording changes which would alleviate the problems. Enter in block 6 any remarks not related to a specific paragraph of the document. If block 7 is filled out, an acknowledgement will be mailed to you within 30 days to let you know that your comments were received and are being considered.

NOTE This form may not be used to request copies of documents, nor to request waivers, deviations, or clarification of specification requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

(Fold along this line)

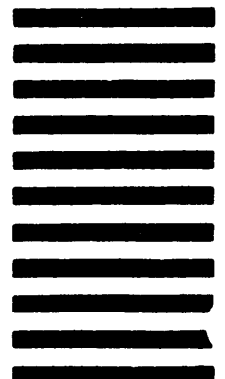*(Fold along this line)*

DEPARTMENT OF THE ARMY

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE $300

BUSINESS REPLY MAIL
FIRST CLASS   PERMIT NO. 12062   WASHINGTON D.C

POSTAGE WILL BE PAID BY THE DEPARTMENT OF THE ARMY

Director
US Army Materiel Command Field Safety Activity
ATTN: AMXOS-SE
Charlestown, IN 47111-9669

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL
(See Instructions · Reverse Side)

1. DOCUMENT NUMBER	2. DOCUMENT TITLE
MIL-HDBK-764(MI)	System Safety Engineering Design Guide for Army Materiel

3a. NAME OF SUBMITTING ORGANIZATION

b. ADDRESS *(Street, City, State, ZIP Code)*

4. TYPE OF ORGANIZATION *(Mark one)*

☐ VENDOR

☐ USER

☐ MANUFACTURER

☐ OTHER *(Specify)*: _____

5. PROBLEM AREAS

a. Paragraph Number and Wording:

b. Recommended Wording:

c. Reason/Rationale for Recommendation:

6. REMARKS

7a. NAME OF SUBMITTER *(Last, First, MI)* – Optional

b. WORK TELEPHONE NUMBER *(Include Area Code)* – Optional

c. MAILING ADDRESS *(Street, City, State, ZIP Code)* – Optional

8. DATE OF SUBMISSION *(YYMMDD)*

DD FORM **1426** 82 MAR   PREVIOUS EDITION IS OBSOLETE.